Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Θωράκιση Συσκευών τύπου Internet of Things (IP Cameras) από Botnets

Σωτήρης Μάρκου

Επιβλέπων Καθηγητής
Δρ. Αδαμαντίνη Περατικού

Μάϊος/ 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Θωράκιση Συσκευών τύπου Internet of Things (IP Cameras) **από** Botnets

Σωτήρης Μάρκου

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάϊος / 2019

Περίληψη

Η Διατριβή αυτή γίνεται στα πλαίσια των ερευνητικών αναγκών του Μεταπτυχιακού Προγράμματος "Ασφάλεια Υπολογιστών και Δικτύων" του Ανοικτού Πανεπιστημίου Κύπρου. Η έρευνα αυτή αποσκοπεί στην μελέτη του τρόπου λειτουργίας των δικτυακών καμερών και συσκευών IoT (Internet of Things) γενικότερα, καθώς κακές πρακτικές οδήγησαν σε παραβιάσεις και επιθέσεις τεραστίων και πρωτόγνωρων διαστάσεων. Η μελέτη των επιθέσεων, του τρόπου εκτέλεσης τους, των εμπλεκόμενων μερών, συνεπειών και ενδεχομένως τρόπων αντιμετώπισης τους σκοπεύει να αποδώσει στην ερευνητική κοινότητα ένα πλαίσιο εργασίας βάση του οποίου οι δικτυακές κάμερες και συσκευές IoT θα μπορούν να δρουν σε ένα ασφαλέστερο περιβάλλον ελαχιστοποιώντας τους κινδύνους επίθεσης και εκμετάλλευσης από botnets.

Ο στόχος αναμένεται να επιτευχθεί μέσω πειραματικής δοκιμής 3 καμερών από διαφορετικούς κατασκευαστές, στις οποίες θα γίνει μια αξιολόγηση κινδύνου έτσι ώστε να εντοπιστούν αδυναμίες και ευπάθειες. Οι ευπάθειες μπορεί να προκύπτουν από τις εγκατεστημένες εφαρμογές και το λειτουργικό σύστημα των καμερών. Στη συνέχεια μέσω αξιολόγησης των κοινών ευπαθειών, εάν αυτές μπορούν να εφαρμοστούν για χρήση σε botnet, θα προταθούν μέτρα αντιμετώπισης και με την χρήση λογισμικού θα μπορεί να γίνεται μια γρήγορη αξιολόγηση επικινδυνότητας σε γενικό επίπεδο.

Καταλήγοντας στα τελικά της συμπεράσματα η μελέτη αυτή αναφέρει τυχόν προβλήματα τα οποία αντιμετώπισε. Επίσης γίνεται αναφορά μελλοντική ερευνητική δραστηριότητα η οποία μπορεί να επιτελεσθεί, στην ανάπτυξη αντιμέτρων, στις απειλές οι οποίες προκύπτουν από την έκθεση συσκευών στο διαδίκτυο και κατ' επέκταση σε hackers.

Summary

This Thesis takes place as part of the research requirements of the Masters Degree in "Computer and Network Security " of the Open University of Cyprus. The research aims to study the working methods of IP cameras and IoT (Internet of Things) devices in general, as bad practices of the past have led to attacks and violations of proportional size and effect. Studying these attacks in the ways they were performed, their comprising parts, their consequences and possibly the methods used to react, aims to provide the research community with a framework based upon which IP Cameras and IoT devices, will be able to work in a safer environment minimizing the attack hazards from botnets.

The goal is expected to be achieved by testing 3 cameras, from different vendors, in a lab environment, upon which a risk assessment will take place in order to identify possible vulnerabilities. Vulnerabilities are expected to occur from the Camera's operating systems and their installed applications. The vulnerabilities, which are common between the 3 cameras, will then be assessed whether they can be used by botnets. Countermeasures will then be proposed while a small software will be developed which will be able to assess the general risk a camera is subjected to.

Concluding the research reports the problems faced during the research while also suggesting future work and further research that can take place in developing countermeasures to the threats that may arise from the cameras exposure to the internet and hackers.

Ευχαριστίες

Με την ολοκλήρωση της Μεταπτυχιακής Διατριβής μου, ολοκληρώνεται επίσης ο κύκλος σπουδών μου στο Μεταπτυχιακό Πρόγραμμα "Ασφάλεια Υπολογιστών και Δικτύων" στο Ανοικτό Πανεπιστήμιο Κύπρου.

Πρωτίστως θέλω να ευχαριστήσω την καθηγήτρια μου Δρ. Αδαμαντίνη Περατικού της οποίας η εξαιρετική καθοδήγηση και στήριξη υπήρξε καθοριστικός παράγοντας στην εκπόνηση της συγκεκριμένης μελέτης. Η έρευνα αυτή μου έδωσε την ευκαιρία να αποκτήσω γνώσεις και εμπειρίες στον τομέα των έξυπνων συσκευών IoT και την ασφάλιση τους. Κατ' επέκταση θέλω επίσης να ευχαριστήσω και τους υπόλοιπους καθηγητές μου Δρ. Στάυρο Σιαηλή υπεύθυνο του Ακαδημαϊκού Προγράμματος, Δρ Κωνσταντίνο Λιμνιώτη και την Δρ Στυλιανή Κλεάνθους των οποίων η διδασκαλία μου μετάφερε την απαραίτητη γνώση για την ολοκλήρωση των σπουδών μου.

Καταλήγοντας θέλω να ευχαριστήσω θερμά την σύζυγο μου για την στήριξη που μου παρείχε κατά την διάρκεια των σπουδών μου, καθώς επίσης και τις επιπλέον οικογενειακές υποχρεώσεις που ανέλαβε για να έχω την ευκαιρία να τις ολοκληρώσω.

ΚΕΦΑΛΑΙΟ 1
Εισαγωγή

Η πρόοδος της τεχνολογίας την τελευταία 10ετία έχει συστήσει την κοινωνία στις έξυπνες συσκευές. Με την έλευση των έξυπνων τηλεφώνων, συσκευών των οποίων πλέον η χρήση περιορίζεται μόνο από την φαντασία του χρήστη τους, έχουν μπει για τα καλά στη ζωή μας οι έξυπνες συσκευές. Οι συσκευές αυτές καλύπτουν ένα ευρύ φάσμα χρήσεων, από τηλεοράσεις μέχρι ψυγεία, και από θερμοστάτες σε ηλεκτρικούς λαμπτήρες και καφετιέρες. Οι συσκευές αυτές μέσω υποστήριξης IP και σύνδεσης στο διαδίκτυο μπορούν να ελεγχθούν απομακρυσμένα μέσω ηλεκτρονικού υπολογιστή, τηλεφώνων ή tablet. Καθώς η πρωταρχική χρήση των συσκευών αυτών δεν είναι η σύνδεση με το διαδίκτυο, πολλές φορές τα θέματα ασφαλείας στο διαδίκτυο δεν λαμβάνονται σοβαρά υπόψη με αποτέλεσμα να αποτελούν εύκολο στόχο για hackers. Οι επίδοξοι hacker επιτιθέμενοι στις συσκευές αυτές εγκαθιστούν botnets δημιουργώντας τεράστιους στρατούς, από μολυσμένες συσκευές, τους οποίους χρησιμοποιούν κυρίως σε DDoS επιθέσεις. Η έρευνα αυτή θα επικεντρωθεί κυρίως στις συσκευές τύπου IP cameras οικιακής χρήσης των οποίων η εκμετάλλευση ελλοχεύει περαιτέρω κινδύνους, πέραν της χρήσης για DDoS επιθέσεις, για την κατασκοπεία – τρομοκρατία των θυμάτων

1.1 Σκοπος

Ο σκοπός της έρευνας είναι να εντοπίσει τα πιο πρόσφατα botnets τα οποία χρησιμοποιούνται σε επιθέσεις συσκευών IoT, τους τρόπους και τις μεθόδους τις οποίες χρησιμοποιούν οι χάκερ για να επιτεθούν στις εν λόγο συσκευές, κατά κύριο λόγο σε IP cameras. Στη συνέχεια θα αναλυθούν οι τρόποι κατά τους οποίους οι συσκευές αυτές τυγχάνουν επίθεσης εκμετάλλευσης και χρήσης από botnets για σκοπούς επιθέσεων ή κατασκοπείας. Μετά την επιτυχή εκμετάλλευση συσκευών της κλάσης αυτής θα προταθούν μέτρα βάση των οποίων θα περιορίζονται οι κίνδυνοι και οι αδυναμίες τους ενώ θα καθοριστεί πλαίσιο ασφαλείας (framework) για την ορθή χρήση και λειτουργία τους.

1.2 ΒΑΣΙΚΑ ΕΡΕΥΝΗΤΙΚΑ ΕΡΩΤΗΜΑΤΑ

Τα βασικά ερευνητικά ερωτήματα τα οποία θα κληθεί να απαντήσει η έρευνα αφορούν τα εξής:

Ποια είναι τα πιο πρόσφατα και πιο διαδεδομένα botnets για IoT συσκευές – κάμερες;

Πως μια διαδικτυακή κάμερα τυγχάνει επίθεσης;

Ποιες είναι οι πιθανές επιπτώσεις από την εκμετάλλευση μιας κάμερας;

Πως μπορεί μια κάμερα να χρησιμοποιηθεί για να αποτελέσει μέρος σε DDoS επίθεση;

Μπορούν μέσω υφιστάμενων μεθόδων ή πρωτοκόλλων να ασφαλιστούν;

1.3 ΑΝΑΓΚΑΙΟΤΗΤΑ ΚΑΙ ΣΠΟΥΔΑΙΟΤΗΤΑ ΤΗΣ ΈΡΕΥΝΑΣ

Η χρήση των δικτυακών καμερών αυξάνεται με εκθετικούς ρυθμούς καθώς χρησιμοποιούνται σαν προσθήκες σε οικιακά συστήματα συναγερμού, παρακολούθησης σε βρεφικά δωμάτια καθώς επίσης και για ερευνητικούς σκοπούς για την συλλογή εικόνας σε εργαστήρια και εργασιακούς χώρους. Οι συσκευές αυτές συνήθως αποτελούν εύκολους στόχους για χάκερ αφενός επειδή οι κατασκευαστές δεν τις θωρακίζουν επαρκώς, και αποτελούν ευάλωτους στόχους, και αφετέρου επειδή οι εκάστοτε χρήστες δεν έχουν τις γνώσεις ή την εμπειρία έτσι ώστε να τις ασφαλίσουν. Ως αποτέλεσμα υπάρχει ένας στρατός για χρήση σε DDoS επιθέσεις από χάκερ, με προκαθορισμένα ονόματα χρήστη και κωδικούς, έτοιμος για χρήση. Παράδειγμα μιας επίθεσης αποτελεί η χρήση του Mirai botnet στις 21 Οκτωβρίου 2016 σε συστήματα του παροχέα υπηρεσιών DNS DYN. Ιστοσελίδες όπως την http://insecam.com/ των οποίων ο σκοπός είναι να φανερώνει κάμερες οι οποίες είναι δημόσια προσβάσιμες με το προκαθορισμένο όνομα χρήστη και τον κωδικό. Ένα πιο δραματικό σενάριο περιγράφεται στο άρθρο “Privacy Nightmare: When baby Monitors go bad” 2015 (Albrecht and McIntyre 2015), όπου χάκερ απέκτησε πρόσβαση στην κάμερα ενός παιδικού δωματίου τρομοκρατώντας τόσο το κοιμώμενο μωρό όσο και τους γονείς του όταν το ανακάλυψαν.

ΚΕΦΑΛΑΙΟ 2
Βιβλιογραφική Επισκόπηση

Καθώς ο τομέας της ασφάλειας και προσπάθειες θωράκισης, τόσο αυτόνομων όσο και ετερώνυμων συστημάτων, έχει τύχει αρκετής προσοχής από τον ερευνητικό κόσμο. Η έρευνα αυτή μέσω επισκόπησης της υφιστάμενης βιβλιογραφίας και μεθόδων, θα προσπαθήσει να εφαρμόσει την υπάρχουσα γνώση στον τομέα των δικτυακών καμερών, εκεί που δεν εφαρμόζεται ήδη, ενώ ενδεχομένως να προτείνει καινούργιες μεθόδους προστασίας.

2.1 ΟΡΙΣΜΟΙ

Στο κομμάτι αυτό η έρευνα θα ασχοληθεί με τον προσδιορισμό των όρων, που την αφορούν και θα χρησιμοποιηθούν στην συνέχεια, όπως έχουν ορισθεί από προηγούμενες ή παραπλήσιες έρευνες έτσι ώστε να μπορεί να προσθέσει στην υφιστάμενη γνώση. Με την πρόοδο της τεχνολογίας, στο μικρό χρονικό διάστημα των 73 χρόνων από την ολοκλήρωση του ENIAC (ενός εκ των πρώτων ηλεκτρονικών υπολογιστών γενικής χρήσης) περάσαμε την εποχή των mainframes, επιτραπέζιων προσωπικών ηλεκτρονικών υπολογιστών, των φορητών ηλεκτρονικών συσκευών τύπου smartphone και tablet. Τώρα μπαίνουμε σιγά σιγά στην εποχή του Internet of Things όπου συσκευές κάθε τύπου αποκτούν πρόσβαση στο δίκτυο και αλληλοεπιδρούν αυτόνομα με το περιβάλλον ανταλλάζοντας δεδομένα, πληροφορίες και εντολές.

2.1.1 INTERNET OF THINGS (IoT)

Η σύγχρονη κοινωνία χαρακτηρίζεται πλέον από τις έξυπνες συσκευές. Έχει μεταβεί από τα έξυπνα τηλέφωνα σε έξυπνους λαμπτήρες, έξυπνα ψυγεία, έξυπνα κλιματιστικά. Η κοινή αντίληψη αποδίδει τον όρο έξυπνη συσκευή σε οποιαδήποτε συσκευή η οποία ενώνεται με το διαδίκτυο και οι λειτουργίες της μπορούν να ελεγχθούν απομακρυσμένα ή μέσω κάποιας εφαρμογής, με ή ακόμα και χωρίς την παρέμβαση του χρήστη. Ο όρος που επικρατεί στην ερευνητική κοινότητα είναι ο “Internet of Things” ο οποίος χρησιμοποιήθηκε για πρώτη φορά το 1999 από τον Kevin Ashton, ο οποίος δούλευε στην προτυποποίηση της κατάταξης αντικειμένων μέσω RFID για λογιστικές εφαρμογές, ενώ η ιδέα της πανταχού παρών επεξεργασίας προϋπήρχε από το 1980 . Ερευνητές έχουν προσπαθήσει να αποδώσουν τον ορισμό του IoT χωρίς όμως να

υπάρξει συμφωνία επ' αυτού. Ο Haller et al πρότεινε ένα ορισμό για IoT ως εξής: "'Ενας κόσμος όπου τα φυσικά αντικείμενα ενσωματώνονται άψογα στο δίκτυο πληροφοριών και γίνονται ενεργά μέλη της επιχειρηματικής δραστηριότητας.". Επεκτείνοντας τον όρο οι Sarma et al ορίζουν τον όρο "Things" από φυσικά σε ιδεατά αντικείμενα που μπορούν να συνδεθούν στο διαδίκτυο. (Weyrich and Ebert 2016). Από την στιγμή που ο ορισμός για το Internet of Things είναι ακόμα υπό εξέλιξη νοείται πως δεν υπάρχουν πρότυπα και κανονισμοί τους οποίους πρέπει να ακολουθούν οι κατασκευαστές για να διασφαλίζεται η διαλειτουργικότητα και συμβατότητα μεταξύ διαφόρετικών συσκευών, όπως επίσης και τα θέματα ασφαλείας τα οποία θα απασχολήσουν την εν λόγο έρευνα. Για τον λόγο αυτό γίνονται προσπάθειες προτυποποίησης του τομέα με 3 διαφορετικές παραλλαγές:

2.1.2 MALWARE

Η πλειονότητα του πληθυσμού εάν ερωτηθεί σχετικά με το τί είναι ένα malware, θα απαντήσει πως πρόκειται περί ιού ο οποίος προσβάλλει τους ηλεκτρονικούς υπολογιστές. Εν μέρει αυτό είναι αλήθεια αλλά για τους σκοπούς της έρευνας πρέπει να αποδοθούν πιο προσδιορισμένοι ορισμοί έτσι ώστε να καθίσταται πιο ακριβής επί του θέματος. Ένας εκ των ορισμών που έχουν ήδη αποδοθεί είναι "Malware είναι επιβλαβές λογισμικό το οποίο εσκεμμένα επιτίθεται σε άλλο λογισμικό, όπου επιβλαβές επίθεση προσδιορίζεται η πρόκληση της συμπεριφοράς του λογισμικού να αλλάξει από την προτιθέμενη συμπεριφορά του. Δυστυχώς όμως η προτιθέμενη συμπεριφορά του λογισμικού σπανίως προσδιορίζεται (Kramer and Bradfield 2010).

2.1.3 BOTNETS

Τα botnets αποτελούν δίκτυα από "bots", δηλαδή μολυσμένα συστήματα τα οποία ελέγχονται απομακρυσμένα από ένα κεντρικό ηλεκτρονικό σύστημα μέσω ενός η και περισσοτέρων συστημάτων ελέγχου. Το κεντρικό ηλεκτρονικό σύστημα είναι αυτό που χρησιμοποιεί ο δράστης για να στείλει τις εντολές οι οποίες στη συνέχεια μεταβιβάζονται μέσω των συστημάτων ελέγχου (Karasaridis, Rexroad, and Hoeflin n.d.). Τα πιο γνωστά botnets τα οποία έχουν χρησιμοποιηθεί σε συσκευές IoT, τα τελευταία χρόνια, για επιθέσεις είναι μεταξύ άλλων είναι το Mirai, το Persirai και το Hajime τα οποία θα δούμε πιο κάτω.

2.1.3.1 MIRAI

Ένα εκ των διασημότερων botnet το οποίο χρησιμοποιείται σε επιθέσεις DDoS με την χρήση IoT συσκευών είναι το Mirai botnet. Το συγκεκριμένο botnet εμφανίστηκε τον Αύγουστο του 2016, ενώ η πρώτη επίθεση με την χρήση του Mirai έγινε τον Σεπτέμβριο του ίδιου χρόνου. Το botnet αυτό ψάχνει για ανοικτή θύρα telnet (23) στις διάφορες συσκευές και στη συνέχεια δοκιμάζει να κάνει brute force attack σε αυτές βασισμένο σε ευρέως γνωστά ονόματα χρηστών / κωδικών. Σε ένα διάστημα 2 μηνών υπήρξαν τουλάχιστον 5 μεγάλες επιθέσεις στο διαδίκτυο. Οι σημαντικότερες εξ αυτών ήταν η επίθεση στην εταιρία "Krebs on Security" με traffic της τάξης των 620 Gbps, ή επίθεση στην εταιρία DYN (παροχέα υπηρεσιών DNS) η οποία επηρέασε υπηρεσίες όπως το twitter, το Github και άλλες, ενώ η επίθεση στον Γαλλικό πάροχο υπηρεσιών cloud OVH κατέγραψε κίνηση μεγέθους 1.2 Tbps (Antonakakis et al. n.d.; Kolias et al. 2017), (Antonakakis et al. n.d.). Από τα μεγέθη τα οποία προαναφέρονται είναι ευκόλως αντιληπτό και το μέγεθος τους προβλήματος ιδιαίτερα από την στιγμή που ο δημιουργός του Mirai δημοσιοποίησε τον πηγαίο κώδικα του με αποτέλεσμα την ταχεία διάδοση του καθώς επίσης και την δημιουργία πολλών και διαφόρων παραλλαγών του.

2.1.3.2 PERSIRAI

Το botnet Persirai χρησιμοποιεί την υποδομή του Mirai αλλά αντί να επιτίθεται στο port 23 χρησιμοποιεί TCP συνδέσεις στο Port 81 στο οποίο απαντούν πολύ συχνά οι IP κάμερες. Στη συνέχεια εγχέονται εντολές στην κάμερα να ενωθεί σε συγκεκριμένες ιστοσελίδες από τις οποίες κατεβάζουν τις περαιτέρω εντολές του botnet. Αφού εκτελεστούν οι εντολές σβήνονται κι έτσι το botnet τρέχει πλέον στη μνήμη RAM της κάμερας έτοιμο πλέον να προσβάλει άλλες κάμερες στο δίκτυο ή να αποτελέσει η ίδια μέρος επίθεσης (Behniafar, Nowroozi, and Shahriari 2018) (Kolias et al. 2017) .

2.1.3.2 HAJIME

Το botnet Hajime (ιαπωνική λέξη για την Αρχή / Μέλλον) έγινε για πρώτη φορά αντιληπτό τον Οκτώβριο του 2016 λίγο μετά την κυκλοφορία του πηγαίου κώδικα του Mirai. Ενώ τα ίχνη στο δίκτυο και η συμπεριφορά αναμετάδοσης προσομοιάζει αυτή του Mirai εν τούτοις το botnet/worm αυτό είναι αρκετά πιο εξελιγμένο καθώς δεν έχουν κεντρικά συστήματα ελέγχου αλλά χρησιμοποιούν τεχνολογία peer-to-peer, όπως αυτή που χρησιμοποιείτε για την ανταλλαγή αρχείων BitTorrent, για την μετάδοση των εντολών και του εκτελέσιμου αρχείου του ιού (Edwards and Profetis 2016). Όπως μπορούμε εύκολα να συμπεράνουμε αυτό δυσχεραίνει το έργο των IDS / IPS συστημάτων καθώς η άρνηση πρόσβασης σε γνωστούς διακομιστές ελέγχου, υφιστάμενη τακτική που εμποδίζει την επικοινωνία των bots με τα κέντρα ελέγχου τους, δεν

μπορούν να εμποδίσουν επιθέσεις από τέτοιου είδους μολυσμένα bots (Botnet and Diaconescu n.d.) .

2.1.4 ΕΠΙΘΕΣΕΙΣ DOS ΚΑΙ DDOS

Οι επιθέσεις DoS υπήρξαν ιδιαίτερα δημοφιλής στο διαδίκτυο από το 1996 και μετά καθώς αποτελούσαν μια δραστική μέθοδο πρόκλησης "ζημιάς" σε παρόχους υπηρεσιών στο διαδίκτυο με ελάχιστη προσπάθεια. Η επίθεση εκμεταλλευόταν αδυναμίες στην σουίτα του πρωτοκόλλου TCP/IP . Η μεθοδολογία που χρησιμοποιείτο ήταν η εξής "Ο επιτιθέμενος έστελνε ένα μεγάλο αριθμό αιτημάτων σύνδεσης TCP, στο θύμα του με ψεύτικη διεύθυνση αποστολέα. Η κάθε αίτηση σύνδεσης έκανε τον στόχο να διοχετεύει τους περιορισμένους πόρους του, με αποτέλεσμα όταν αυτοί εξαντλούνταν το θύμα δεν μπορούσε πλέον να εξυπηρετήσει κανονικές και έντιμες προσβάσεις"(Schuba et al. 1997)
Η πρώτη καταγεγραμμένη επίθεση DDoS έγινε κατά την πρώτη εβδομάδα του Φεβρουαρίου του 2000 όταν ο χάκερ "mafiaboy" ένας 15χρονος Καναδός οργάνωσε μια σειρά από DoS επιθέσεις ενάντια σε ιστοσελίδες διαδικτυακού εμπορίου συμπεριλαμβανομένου της Amazon και eBay. Χρησιμοποιώντας ηλεκτρονικούς υπολογιστές από διάφορες τοποθεσίες με τους οποίους υπερφόρτωσε τους διακομιστές των παρόχων κατάφερε να επιφέρει ζημιές πέραν του 1.7 δισεκατομμυρίων δολαρίων στις επιχειρήσεις αυτές (denial of service attack | Definition & Facts | Britannica.com n.d.).

2.2 ΕΠΙΘΕΣΕΙΣ IoT.

Έχοντας καταγράψει την αντίληψη του ερευνητικού κοινού όσον αφορά τους ορισμούς που θα χρησιμοποιηθούν, η έρευνα καταγράφει την παρούσα κατάσταση όσον αφορά τις επιθέσεις, μέτρα ασφαλείας αλλά και αδυναμίες στις οποίες υπόκεινται οι συσκευές τύπου IoT. Με την διάδοση του botnet Mirai που αναφέρθηκε πιο πάνω, σε σύντομο χρονικό διάστημα πραγματοποιήθηκαν διάφορες DDoS επιθέσεις. Προς απόδειξη της σπουδαιότητας της έρευνας οι επιθέσεις αυτές αναφέρονται πιο κάτω:

2.2.1 ΕΠΙΘΕΣΗ OVH.

Η εταιρία OVH αποτελεί μια Γαλλική εταιρία παροχής υπηρεσιών cloud computing με υπηρεσίες όπως web hosting, web services, με αφιερωμένους αποκλειστικούς server και Ιδεατούς server (VPS – Virtual Private Servers). Στις 22 Σεπτεμβρίου 2016 οι διακομιστές της εταιρίας έτυχαν μιας σειράς επιθέσεων DDoS οι οποίες σε αρκετές περιπτώσεις ξεπερνούσαν τα 100 Gbps σε συγκεκριμένο server ενώ η μεγαλύτερη καταγεγραμμένη επίθεση σε συγκεκριμένο server έφτασε μέχρι και 799 Gbps. Το σύνολο των επιθέσεων δημιούργησε εξωφρενική κίνηση δικτύου η οποία κυμαινόταν από 1.1Tbps μέρι 1.5Tbps η οποία παράχθηκε από 145607 botnets (δικτυακές κάμερες και ψηφιακούς σταθμούς πολυμέσων) (Angrishi 2017). Αυτή αποτέλεσε μια από τις πρώτες επιθέσεις με την χρήση του botnet Mirai η οποία έδειξε στον κόσμο το μέγεθος της ζημιάς η οποία μπορεί να επέλθει από την άγνοια λήψης μέτρων προστασίας σε απλές και φαινομενικά αθώες οικιακές συσκευές τύπου Internet of Things (IoT).

2.2.2 ΕΠΙΘΕΣΗ DYN.

Η εταιρία DYN πραγματεύεται μεταξύ άλλων την παροχή υπηρεσιών DNS (Domain Name Services). Αποτελεί μια από τις μεγαλύτερες εταιρίες παροχής υπηρεσιών DNS στον κόσμο, εν τούτοις υπέστηκε αρκετά προβλήματα μετά από την επίθεση που δέχτηκε στις 21 Οκτωβρίου 2016 στους DNS Server της από πέραν των 100000 IoT συσκευές. Η επίθεση και πάλι πραγματοποιήθηκε με την χρήση του Mirai και στόχευε DDoS σε TCP και UDP θύρες 53 που χρησιμοποιεί το πρωτόκολλο DNS. Το μέγεθος της καταγεγραμμένης επίθεσης ξεπέρασε το 1.2Tbps αν και δεν επιβεβαιώθηκε από την DYN (Angrishi 2017). Η επίθεση αυτή προξένησε αρκετά προβλήματα στους πελάτες της DYN όπως την Amazon, Spotify, Reddit και άλλες, οι οποίες κατέστησαν μερικώς ή και μη διαθέσιμες προς τους πελάτες τους.

2.2.3 ΟΙΚΙΑΚΕΣ ΕΠΙΘΕΣΕΙΣ

Αν και στις 2 πιο πάνω περιπτώσεις επιθέσεων είδαμε τα μεγέθη των ζημιών που μπορεί να επέλθουν από την εκμετάλλευση των συσκευών IoT στην βιομηχανία, εν τούτοις ένα ακόμα πιο ενοχλητικό κομμάτι ταλανίζει τους ιδιοκτήτες των συσκευών αυτών. Η εκμετάλλευση τους από επιτήδειους hacker αποτελεί κίνδυνο τόσο προς την ιδιωτικότητα των χρηστών όσο και το αίσθημα της ασφάλειας τους . Υπάρχουν περιπτώσεις όπου δικτυακές κάμερες ενδεχομένως λόγο χρήσης αδύνατων κωδικών τυγχάνουν εκμετάλλευσης από hackers οι οποίοι μπορούν να "παρατηρούν" τα θύματα. Η χειρότερη δε των περιπτώσεων αποτελεί την εκμετάλλευση που καταγράφεται στο άρθρο "Privacy Nightmare: When Baby Monitors Go Bad" (Albrecht and McIntyre 2015). Οι γονείς Adam και Heather Schreck άκουγαν φωνές από το υπνοδωμάτιο του παιδιού τους όπου είχαν εγκατεστημένη δικτυακή κάμερα για να το προσέχουν. Με την είσοδο τους στο δωμάτιο ο hacker άρχισε να φωνάζει βωμολοχίες προς τους γονείς που αφού κατάλαβαν το τι συνέβαινε αποσύνδεσαν την ηλεκτροδότηση στην κάμερα. Η περίπτωση αυτή θα μπορούσε να είχε και χειρότερες εκβάσεις στην περίπτωση που το παιδάκι ήταν ξύπνιο και κατανοούσε το τι του έλεγε ο δράστης.

2.3 ΥΦΙΣΤΑΜΕΝΕΣ ΈΡΕΥΝΕΣ.

Σε αυτό το στάδιο η έρευνα θα επικεντρωθεί στην αναθεώρηση άλλων ερευνών οι οποίες έχουν διεκπεραιωθεί σχετικά με την ασφάλεια των δικτυακών καμερών. Καθώς ο τομέας της ασφάλειας τον χώρο της τεχνολογίας και των πληροφοριακών συστημάτων κινείται με γοργούς ρυθμούς έχει ληφθεί η απόφαση όπως η ανασκόπηση γίνει σε έρευνες των τελευταίων 3 χρόνων. Αυτό αναμένεται να βοηθήσει στην αξιολόγηση του πως η μαζικές επιθέσεις μεγεθών 1.2 Terabits per second με την χρήση IoT συσκευών, έχουν επηρεάσει τόσο την ερευνητική κοινότητα, όπως επίσης και την βιομηχανία η οποία κινείται στο υπόβαθρο της κατασκευής και διάθεσης δικτυακών καμερών.

Όπως αναφέρθηκε πιο πάνω μετά την εκδήλωση του Mirai και των παραλλαγών του έγινε αντιληπτή η επιτακτική ανάγκη θωράκισης της ασφάλειας των συστημάτων τα οποία απαρτίζουν τις IoT συσκευές . Καινούργιες συσκευές ή αναβαθμίσεις στο firmware συσκευών έκλειναν την θύρα 23 και την υπηρεσία telnet από αρκετά μοντέλα συσκευών χωρίς αυτό να τις καθιστά άτρωτες σε επιθέσεις από botnets. Αν και στο στάδιο συγγραφής της έρευνας δεν έχει γίνει αντιληπτό σχετικό botnet, θεωρείται πως αδυναμίες που εντοπίστηκαν στους webserver δικτυακών καμερών , όπως την εκτέλεση απομακρυσμένου κώδικα (remote code execution) (Seralathan et al. 2018), μπορούν αρκετά εύκολα να αυτοματοποιηθούν και να κωδικοποιηθούν σε μορφή botnet. Πλέον μέσω απλών ελέγχων στη βάση δεδομένων CVE (Common

Vulnerabilities and Exposure), όπου καταγράφονται οι αδυναμίες που έχουν τα λειτουργικά συστήματα και εφαρμογές, μπορεί εύκολα να δημιουργηθεί μια λίστα με συγκεκριμένες αδυναμίες που ενδεχομένως να έχουν κοινές συγκεκριμένα μοντέλα κάποιων κατασκευαστών(Bugeja, Jönsson, and Jacobsson 2018). Εάν η εκμετάλλευση συγκεκριμένης αδυναμίας μπορεί να αυτοματοποιηθεί με την χρήση κώδικα, τότε μπορεί να δημιουργηθεί το ανάλογο botnet. Το γεγονός πως μηχανές αναζήτησης IoT συσκευών όπως η shodan.io έχουν δυνατότητες αναζήτησης συγκεκριμένου τύπου συσκευών, με κριτήρια που αφορούν τόσο τον κατασκευαστή όσο και συγκεκριμένες ιδιαιτερότητες της συσκευής (π.χ. έκδοση webserver ή υποστήριξη rtsp) περιορίζουν τη λίστα αρκετά ως προς τους επίδοξους στόχους που μπορεί να έχει το συγκεκριμένο botnet. Το γεγονός δε πως η χρήση της μηχανής αναζήτησης μπορεί να ενσωματωθεί σε λογισμικό μέσω API μπορεί να κάνει την εξάπλωση των botnets πιο στοχευμένη και κατά συνέπεια λιγότερο αντιληπτή από τείχη προστασίας και IDS συστήματα. Αναλόγως κατασκευαστή και μοντέλου δικτυακές κάμερες υποστηρίζουν τα πρωτόκολλα rtsp, στο οποίο αν δεν εφαρμοστεί ταυτοποίηση χρήστη, μπορεί να χρησιμοποιηθεί σε δύο ειδών επιθέσεις, αφ ' ενός για παραβίαση της ιδιωτικότητας του ιδιοκτήτη υποκλέπτοντας την εικόνα της κάμερας(Seralathan et al. 2018). Η δεύτερη επίθεση που μπορεί να πραγματοποιηθεί οφείλεται στο γεγονός πως το rtsp χρησιμοποιεί το πρωτόκολλο μετάδοσης UDP συνεπώς καταγράφοντας αρκετά δεδομένα ένας επιτιθέμενος μπορεί να προσβάλει την ακεραιότητα της εικόνας στέλνοντας αναχρονολογημένη εικόνα στον δέκτη/χρήστη παριστάνοντας την κάμερα (Boyarinov and Hunter 2017). Οι τύποι αυτών των επιθέσεων είναι εκτός του αντικειμένου της έρευνας η οποία δεν θα εμβαθύνει περαιτέρω.

Όπως προαναφέρθηκε οι κατασκευαστές έχουν αρχίζει να εφαρμόζουν μέτρα ασφαλείας στα προϊόντα δικτυακών καμερών χωρίς ωστόσο να έχει καθοριστεί ένα πρότυπο. Προσπάθειες ασφάλισης των δικτυακών καμερών θέλουν τις κάμερες να λαμβάνουν τις ρυθμίσεις τους κεντρικά από τους διακομιστές του κατασκευαστή αφού πρώτα κάμερα και χρήστης συνδεθούν στο διαδίκτυο και κατά συνέπεια μεταξύ τους μέσω του λογισμικού του κατασκευαστή. Αυτό φυσικά ελλοχεύει τους δικούς του κινδύνους καθώς hackers μπορούν να πραγματοποιήσουν Man in the Middle attacks οι οποίες μπορούν με την σειρά τους να πλήξουν διαφορετικές πτυχές της ασφάλειας. Πέραν της προσβολής της ακεραιότητας δεδομένων έρευνα έχει δείξει πως πολλές φορές οι εφαρμογές κινητών τηλεφώνων έχουν αποθηκευμένα ή και στέλνουν τα διαπιστευτήρια της κάμερας σε κανονικό κείμενο χωρίς να έχουν κρυπτογραφηθεί (Boyarinov and Hunter 2017). Αυτό μπορεί να δώσει πρόσβαση στον επίδοξο επιτιθέμενο.

2.4 ΑΞΙΟΛΟΓΗΣΗ ΕΥΡΗΜΑΤΩΝ.

Οι έρευνες που έχουν πραγματοποιηθεί μέχρι σήμερα έχουν δώσει αρκετή διορατικότητα στις πολλές αδυναμίες σε θέματα ασφάλειας που διέπουν τις δικτυακές κάμερες και τις συσκευές IoT γενικά. Υπήρξαν ερευνητές που έκαναν επιτυχή επιθέσεις σε δικτυακές κάμερες προς απόδειξη των αδυναμιών τους (Boyarinov and Hunter 2017)(Tekeoglu and Tosun 2015). Άλλοι ερευνητές με την χρήση δημόσια διαθέσιμων εργαλείων έδειξαν την ευκολία με την οποία μπορείς να βρεις διαθέσιμους στόχους προς επίθεση (Bugeja, Jönsson, and Jacobsson 2018) αποδεικνύοντας πως οι επίδοξοι εισβολείς ενδεχομένως να περάσουν απαρατήρητοι από συστήματα ασφαλείας δικτύων και παρόχων υπηρεσιών διαδικτύου. Βάση των ερευνών αυτών βλέπουμε σιγά σιγά τους κατασκευαστές να εφαρμόζουν μέτρα ασφαλείας στις συσκευές τους. Αποτρέποντας μη ασφαλή πρωτόκολλα στις συσκευές τους, χωρίς όμως να έχει καθοριστεί ένα πρότυπο κανόνων ασφαλείας ή καλών πρακτικών οι οποίες να τίθενται αυτόματα σε εφαρμογή, έτσι ώστε να προστατεύουν ακόμα και τους πιο αδαή, σε θέματα ασφαλείας ηλεκτρονικών υπολογιστών, χρήστες από επιθέσεις. Είναι ευρέως αποδεκτό πως ο τομέας ασφάλειας πληροφοριακών συστημάτων και κατ' επέκταση IoT συσκευών είναι ευμετάβλητος συνεπώς το οποιοδήποτε πρότυπο πρέπει να είναι ευέλικτο έτσι ώστε να μπορεί να προστατεύεται και από επιθέσεις οι οποίες δεν έχουν γίνει ακόμα αντιληπτές ή που δεν υπάρχουν ακόμα διαθέσιμα τα μέσα υλοποίησης τους (πχ σπάσιμο του κρυπτογραφικού αλγόριθμου που ενδεχομένως να χρησιμοποιεί μια δικτυακή κάμερα).

2.5 ΑΙΤΙΟΛΟΓΗΣΗ – ΑΝΑΓΚΑΙΟΤΗΤΑ ΈΡΕΥΝΑΣ

Καθώς άλλες έρευνες έχουν ασχοληθεί με τον εντοπισμό και εκμετάλλευση αδυναμιών σε δικτυακές κάμερες, η έρευνα αυτή προτίθεται να ερευνήσει την πρόοδο σε θέματα ασφαλείας που έχουν κάνει διάφοροι κατασκευαστές μέχρι σήμερα. Εάν διαπιστωθεί πως είναι εφαρμόσιμη θα γίνει απόπειρα επίθεσης με το Mirai botnet για τη συλλογή δεδομένων κατά την διάρκεια και την ολοκλήρωση της επίθεσης. Στην συνέχεια θα κατηγοριοποιήσει τις αδυναμίες, τις οποίες ενδεχομένως να διέπουν κάποιες από τις μάρκες ή μοντέλα τα οποία θα τύχουν εξέτασης, ανάλογα με τον τομέα τον οποίο πλήττουν πχ λειτουργικότητα, ιδιωτικότητα ή αξιοπιστία. Στη συνέχεια θα γίνει έλεγχος ποιες από αυτές τις αδυναμίες ενδέχεται να μπορούν να κωδικοποιηθούν σε μορφή script και κατά συνέπεια να συσταθούν σαν αυτόνομο botnet το οποίο να ψάχνει και να προσβάλει παρόμοιες συσκευές στο διαδίκτυο μέσω των προαναφερθέντων μηχανών αναζήτησης IoT.

ΚΕΦΑΛΑΙΟ 3
Μεθοδολογία

Όπως συμβαίνει με την ανάπτυξη λογισμικού έτσι και ο τομέας της ασφάλειας χρήζει συνεχούς ανάπτυξης, βελτίωσης και επίλυσης προβλημάτων. Θεωρείται έτσι λογικό όπως η έρευνα μελετήσει και αναλύσει κάποια από τα μοντέλα κύκλου ζωής των λογισμικών και εφαρμόσει τις αρχές τους τόσο στην αναζήτηση των αδυναμιών όσο και στην πρόταση μέτρων αντιμετώπισης τους. Αυτό θα βοηθήσει μελλοντικές έρευνες στην αντίληψη του κύκλου εργασιών που διεκπεραιώθηκαν καθώς επίσης και τις εργασίες που εναπομένουν σε μελλοντικούς ερευνητές για υλοποίηση.

3.1 WATERFALL MODEL

Το μοντέλο καταρράκτη στην ανάπτυξη λογισμικού αποτελείται από 6 στάδια τα οποία επαναλαμβάνονται κατά την διάρκεια ζωής του λογισμικού και είναι τα ακόλουθα

3.1.1 ΑΠΑΙΤΗΣΕΙΣ

Στο στάδιο αυτό μαζεύονται οι ανάγκες τις οποίες καλείται το λογισμικό να καλύψει. Καταγράφονται τα προβλήματα τα οποία αντιμετωπίζονται και για τα οποία το λογισμικό πρέπει να παρέχει λύση. Στην παρούσα έρευνα αυτό αντιστοιχεί με τις προτάσεις μέτρων προστασίας δικτυακών καμερών με ελάχιστη παρέμβαση από τον χρήστη, όπως έλεγχος ποιότητας κωδικών για απομακρυσμένη πρόσβαση, κλείσιμο ευάλωτων θυρών δικτύου, κρυπτογράφηση δεδομένων.

3.1.2 ΑΝΑΛΥΣΗ

Στο στάδιο αυτό γίνεται η ανάλυση των απαιτήσεων και καθορίζονται λεπτομερώς τόσο το πρόβλημα προς αντιμετώπιση όσο και η προτεινόμενη λύση. Στο σημείο αυτό καθορίζεται αν η λύση είναι εφικτή και εντός προϋπολογισμού. Στην περίπτωση που επιλεγεί αυτή η προσέγγιση θα γίνει η ανάλυση των προβλημάτων που αντιμετωπίζουν οι δικτυακές κάμερες όπως χρήση αδύνατων κωδικών από τους χρήστες, χρήση του telnet για σκοπούς διαχείρισης ή tftp για σκοπούς αναβάθμισης κτλ. Επίσης θα γίνει η αρχική πρόταση μέτρων όπως κλείσιμο της θύρας 23 (telnet), εξαναγκασμός χρήσης ισχυρού κωδικού για την ενεργοποίηση όλων των λειτουργιών της κάμερας, κρυπτογράφηση επικοινωνίας με mobile applications.

3.1.3 ΣΧΕΔΙΑΣΜΟΣ

Κατά τη διάρκεια της φάσης του σχεδιασμού του μοντέλου καταρράκτη γίνονται οι απαραίτητες ενέργειες για να γίνει επακριβώς ο σχεδιασμός της λύσης, στην περίπτωση της έρευνας ο τρόπος επίθεσης στις κάμερες – συλλογή στοιχείων – πρόταση -εφαρμογή αντιμέτρων. Καθορίζεται κατά πόσο ο σχεδιασμός θα γίνει με βάση τις ενέργειες που θα λαμβάνονται σε κάθε φάση ή αν η όλη διαδικασία θα δρομολογείται με βάση τα δεδομένα που θα λαμβάνονται ανά πάσα στιγμή.

3.1.4 ΕΦΑΡΜΟΓΗ

Το στάδιο αυτό αποτελεί την υλοποίηση της λύσης της οποίας σχεδιάστηκε. Στην περίπτωση της υφιστάμενης έρευνας αυτό θα σήμαινε την εκμετάλλευση των διάφορων αδυναμιών στις οποίες υπόκεινται οι διάφορες IP Cameras, λεπτομερής καταγραφή των διαδικασιών που ακολουθήθηκαν καθώς επίσης και των ζημιών οι οποίες μπορεί να προκληθούν από τις ενέργειες οι οποίες λαμβάνονται ανά πάσα στιγμή. Αυτό θα βοηθήσει το επόμενο στάδιο το οποίο αποτελεί την συντήρηση.

3.1.5 ΣΥΝΤΗΡΗΣΗ

Το στάδιο της συντήρησης αποτελεί το μεγαλύτερο και πιο σημαντικό κομμάτι του μοντέλου κύκλου ζωής λογισμικού καθώς από το στάδιο αυτό δίδεται η δυνατότητα επιστροφής σε οποιοδήποτε από τα προηγούμενα στάδια προς διόρθωση λαθών που έγιναν κατά τη διάρκεια τους, τυχόν αλλαγές ή επιπρόσθετες απαιτήσεις από ένα λογισμικό. Στην περίπτωση της έρευνας αυτό εξυπακούει την ανάλυση καινούργιων ή κρυμμένων exploits στα οποία υπόκεινται οι δικτυακές κάμερες.

3.1.6 ΑΠΟΣΥΡΣΗ

Κατά το στάδιο της απόσυρσης το λογισμικό έχει ήδη τελειώσει τον κύκλο είτε γιατί η ανάγκη η οποία κλήθηκε να εξυπηρετήσει δεν υφίσταται πλέον ή έχει απαρχαιωθεί λόγο της προόδου της τεχνολογίας. Γίνεται πλέον η αντικατάσταση του από πιο αποδοτικό λογισμικό με περισσότερες δυνατότητες. Στον τομέα της παρούσας έρευνας αυτό θα σήμαινε πως έχει αλλάξει πλήρως ο τρόπος προσέγγισης μια κυβερνοεπίθεσης λόγο της εφαρμογής μέτρων ασφαλείας βάση των οποίων οι επιθέσεις που περιγράφονται πλέον δεν υφίστανται (Schach 2017).

3.2 ΣΠΕΙΡΟΕΙΔΕΣ ΜΟΝΤΕΛΟ

Το σπειροειδές μοντέλο προσεγγίζει διαφορετικά τον κύκλο ζωής λογισμικού. Η έρευνα θα εξετάσει το μοντέλο αυτό στην προσπάθεια εφαρμογής της καλύτερης προσέγγισης ως προς την εκμετάλλευση και επίλυση των exploits τα οποία ταλανίζουν τις δικτυακές κάμερες. Το σπειροειδές μοντέλο από τον σχεδιασμό του ελαχιστοποιεί τα ρίσκα κατά την διάρκεια της υλοποίησης καθώς η αρχή του κάθε κύκλου στην σπείρα αποτελείται από μια ανάλυση κινδύνου. Η ελαχιστοποίηση των κινδύνων όμως καθώς και η μελέτη εναλλακτικών λύσεων σε αρκετές περιπτώσεις αυξάνει τόσο το κόστος όσο και τον χρόνο υλοποίησης πράγμα το οποίο ενδέχεται να απογοητεύσει τους "πελάτες" του λογισμικού. Η ανάλυση των φάσεων πιο κάτω και η πιθανή εφαρμογή τους στην έρευνα θα δείξει κατά πόσο το εν λόγο μοντέλο είναι το καταλληλότερο για να εφαρμοστεί για τους σκοπούς του πειράματος το οποίο θα διενεργηθεί.

3.2.1 ΣΤΟΧΟΙ

Η κάθε φάση του σπειροειδές μοντέλου γίνεται με γνώμονα τους στόχους και τα επιμέρους προβλήματα τα οποία αναμένεται να λυθούν στο τέλος του κύκλου της σπείρας. Κατά την διάρκεια της στοχοθεσίας περιγράφεται ο τρόπος υλοποίησης των απαιτήσεων, τυχόν εναλλακτικές μεθόδοι επίτευξης των στόχων καθώς επίσης και οι περιορισμοί – προβλήματα τα οποία ενδέχεται να αντιμετωπιστούν.

3.2.2 ΓΡΗΓΟΡΗ ΠΡΩΤΥΠΟΠΟΙΗΣΗ

Στη φάση αυτή δημιουργείται στα γρήγορα μια πρότυπη λύση της οποίας σκοπός είναι η επαλήθευση της κατανόησης των απαιτήσεων. Εννοείται πως το πρωτότυπο αυτό δεν είναι σε λειτουργήσιμη κατάσταση και υπάρχουν αρκετές ευπάθειες και αδυναμίες εν τούτοις χρησιμοποιείται για να αποδειχτεί πως οι απαιτήσεις έχουν γίνει κατανοητές και υπάρχει η κατευθυντήρια γραμμή που θα μας οδηγήσει στην ολοκλήρωση τους. Όπως όλες οι φάσεις του Σπειροειδές μοντέλου έτσι και αυτή ακολουθείται από μια φάση επαλήθευσης και μια φάση ανάλυσης του κίνδυνου υλοποίησης της προτεινόμενης λύσης.

3.2.3 ΠΡΟΔΙΑΓΡΑΦΕΣ

Η επόμενη φάση του Σπειροειδές μοντέλου μας φέρνει στον καθορισμό των Προδιαγραφών του έργου το οποίο έχει ανατεθεί. Βασισμένο στο πρωτότυπο το οποίο έχει ήδη δημιουργηθεί η φάση αυτή επιχειρεί να καταγράψει λεπτομερώς τις απαιτήσεις των χρηστών από το σύστημα, τις διεργασίες και δυνατότητες του συστήματος όπως επίσης και τυχόν περιορισμούς στους

οποίους πρέπει ή ενδεχομένως να υπόκειται. Όπως προαναφέρθηκε έτσι και σε αυτό τον κύκλο του σπυροείδές μοντέλου έρχεται μια φάση επαλήθευσης και μια φάση ανάλυσης κινδύνου.

3.2.4 ΣΧΕΔΙΑΣΜΟΣ

Ο φάση του σχεδιασμού ενός συστήματος δεν διαφέρει ασχέτως με το μοντέλο κύκλου ζωής το οποίο θα επιλεγεί. Έτσι και στο σπειροειδές μοντέλο σε αυτή τη φάση πρέπει να γίνει ο λεπτομερής σχεδιασμός του συστήματος χωρίζοντας το σε μικρότερα πιο διαχειρίσιμα κομμάτια. Η φάση του σχεδιασμού θα καθορίσει τις διάφορες κλάσεις και λειτουργίες του συστήματος καθώς επίσης και την αλληλεπίδραση των διαφόρων μερών του συστήματος. Στη συνέχεια ακολουθούν η φάση της επαλήθευσης του σχεδιασμού όπως επίσης και η ανάλυση κινδύνου σχετικά με τις επιλογές τις οποίες έχουν γίνει στη φάση του σχεδιασμού.

3.2.5 ΥΛΟΠΟΙΗΣΗ

Όπως και στον σχεδιασμό έτσι και στην Υλοποίηση δεν υπάρχουν διαφορές με τα υπόλοιπα μοντέλα. Οι προγραμματιστές ακολουθώντας τον σχεδιασμό υλοποιούν ξεκινούν την δημιουργία του ολοκληρωμένου συστήματος, δοκιμάζοντας παράλληλα την ορθή λειτουργία του. Με το πέρας της υλοποίησης επέρχεται για τελευταία φορά η φάση της επαλήθευσης της ορθότητας του συστήματος όπως επίσης και η τελική ανάλυση κινδύνου της οποίας το έργο είναι να προκαταλάβει πιθανά προβλήματα κατά την φάση της ενσωμάτωσης.

3.2.6 ΕΝΣΩΜΑΤΩΣΗ

Το σύστημα σε αυτή την φάση είναι τελειωμένο και έτοιμο να μπει σε live περιβάλλον. Λαμβάνονται τα απαραίτητα μέτρα διασφάλισης της ελάχιστης περιόδου μη διαθεσιμότητας του συστήματος ενώ γίνονται τυχόν μεταφορές δεδομένων ανάμεσα στο παλαιό και καινούργιο σύστημα.

3.3 AGILE PROCESSES MODEL

Το μοντέλο ανάπτυξης λογισμικού Agile Processes αποτελεί μια γκρίζα περιοχή στην επιστήμη της Τεχνολογίας Λογισμικού καθώς θεωρεί το προϊόν πολύ πιο σημαντικό από την ανάλυση και τεκμηρίωση του. Αυτό δίνει την δυνατότητα σε αυτό το μοντέλο να είναι αρκετά πιο γρήγορο στην παράδοση κομματιών ενός συστήματος και στη συντήρηση τους, εν τούτοις όμως δεν είναι τόσο αξιόπιστο καθώς υπόκειται αρκετές φορές σε λάθη τόσο στον σχεδιασμό τον κομματιών όσο και της υλοποίησης. Αν και δεν έχουν αποτιμηθεί σαν καλή ή κακή πρακτική διατήρησης του κύκλου ζωής ενός λογισμικού ή έργου, η μέθοδος αυτή έχει μεγαλύτερα ποσοστά επιτυχίας όταν οι απαιτήσεις δεν είναι ξεκάθαρες, αλλάζουν εύκολα και ο χρόνος αντιμετώπισης / επίλυσης τους πρέπει να είναι άμεσος.
Στον τομέα της Ασφάλειας Πληροφοριακών Συστημάτων και κατ' επέκταση της έρευνας αυτής, η οποία επιζητά την θωράκιση των δικτυακών καμερών και συσκευών IoT η μέθοδος αυτή φαίνεται η καταλληλότερη. Υπάρχουν πάρα πολλές υφιστάμενες απειλές ενώ συνεχώς ανακαλύπτονται καινούργιες και χρειάζεται η ανάπτυξη μεθόδων που θα μπορούν άμεσα να μετριάζουν τα αποτελέσματα μιας πιθανής εκμετάλλευσης αδυναμίας ενώ παράλληλα σε σύντομο χρονικό διάστημα να γίνεται η αντιμετώπιση και επίλυση της ευπάθειας.

Υπήρξε εμπειρία κατά την διάρκεια της έρευνας όπου κατά την περιγραφή και καθορισμό στόχων του πειράματος, που περιείχε επίθεση με την χρήση του botnet Mirai στις δικτυακές κάμερες, έπρεπε να γίνει ριζική αλλαγή καθώς οι ευπάθειες που σχετίζονταν με το συγκεκριμένο botnet ήδη αντιμετωπίστηκαν από τους κατασκευαστές. Συνεπώς η πειραματική δοκιμή έπρεπε να σχεδιαστεί εκ νέου. Στην περίπτωση χρήσης μοντέλων ανάπτυξης λογισμικού τα οποία απαιτούν εκτενή τεκμηρίωση και καταγραφή των συγκεκριμένων ευπαθειών, η πειραματική δοκιμή να καταστήσει την έρευνα εκπρόθεσμη.

Κεφάλαιο 4
Σχεδιασμός Πειράματος

Το κεντρικό στοιχείο της έρευνας είναι η θωράκιση των δικτυακών καμερών από επιθέσεις botnet. Για να επιτευχθεί όμως ο στόχος αυτός θα πρέπει να προσφερθεί μια όσον το δυνατό πιο ολοκληρωμένη λύση η οποία να αποτρέπει την εκμετάλλευση των καμερών τόσο από botnets όσο και από χειροκίνητες επιθέσεις από επιτιθέμενους. Συνεπώς η έρευνα θα ασχοληθεί με τις πιο κοινές επιθέσεις τις οποίες μπορεί να δεχθεί μια IoT συσκευή σε ένα κλειστό και ελεγχόμενο περιβάλλον, προτείνοντας παράλληλα μέτρα αντιμετώπισης τους. Στη συνέχεια θα πραγματοποιηθεί επίθεση με το Mirai botnet για έλεγχο της ασφάλειας και επαλήθευση. Δια τον λόγο αυτό προτείνεται πιο κάτω η εξής διαρρύθμιση εργαστηρίου στο οποίο θα πραγματοποιηθεί το πείραμα της έρευνας.

4.1 HARDWARE REQUIREMENTS – ΑΠΑΙΤΗΣΕΙΣ ΥΛΙΣΜΙΚΟΥ

Για την δημιουργία του εργαστηρίου η έρευνα θα αξιοποιήσει το ακόλουθο εργαστηριακό περιβάλλον για τον περιορισμό τον συσκευών που θα εξεταστούν, και την αποτροπή επέκτασης των συνεπειών των δοκιμών εκτός του χώρου του εργαστηρίου.

4.1.1 SWITCH

Για την υλοποίηση του πειράματος η έρευνα αυτή θα αξιοποιήσει ένα Layer 2 managed switch από την HP μοντέλου «HP Procurve 1800-24G» Το switch αυτό διαθέτει 24 1Gbps θύρες ενώ υποστηρίζει την δημιουργία vlans και Port Mirroring (SPAN Ports) πράγμα που το καθιστά αρκετό για τους σκοπούς του πειράματος. Οι δικτυακές κάμερες θα τοποθετηθούν σε ξεχωριστό vlan στο switch και οι θύρες στις οποίες είναι ενωμένες θα γίνονται mirror στον ηλεκτρονικό υπολογιστή ο οποίος μέσω wireshark ή tcpdump θα συλλέγει τα ωμά δεδομένα από όλα τα στοιχεία του.

4.1.2 ΔΙΚΤΥΑΚΕΣ ΚΑΜΕΡΕΣ

Για σκοπούς αξιοπιστίας των αποτελεσμάτων της έρευνας έχουν επιλεχθεί 3 ξεχωριστά μοντέλα δικτυακών καμερών από διαφορετικούς κατασκευαστές και με διαφορετικό τρόπο λειτουργίας. Αναμένεται έτσι πως τα αποτελέσματα που θα εξαχθούν θα είναι αμερόληπτα και αξιόπιστα καθώς δεν θα εκτίθεται συγκεκριμένος κατασκευαστής. Στην περίπτωση που οι αδυναμίες (vulnerabilities) επηρεάζουν όλους τους κατασκευαστές η έρευνα μπορεί να εξάγει τα δικά της συμπεράσματα ως προς τον τρόπο χειρισμού του τομέα ασφαλείας των κατασκευαστών δικτυακών καμερών. Στις πλείστες περιπτώσεις το firmware των δικτυακών καμερών αποτελείται από κάποια διανομή busybox linux η οποία παραμετροποιείται για χρήση σε συγκεκριμένη κάμερα. Αν και δεν υπάρχουν στοιχεία άμεσα διαθέσιμα στο διαδίκτυο, η μόνη ένδειξη σχετικά με την χρονολογία κατασκευής και διάθεσης των κάμερών στις αγορές, ο μόνος τρόπος απόκτησης μιας ενδεικτικής ημερομηνίας είναι η ημερομηνία έκδοσης του Πιστοποιητικού Συμμόρφωσης με την Ευρωπαϊκη Νομοθεσία και οδηγίες (CE Mark or Declaration of Conformity). Αυτό το στοιχείο θα χρησιμοποιηθεί ως ένδειξη της ημερομηνίας κυκλοφορίας των καμερών που θα εξεταστούν. Οι κάμερες οι οποίες θα χρησιμοποιηθούν για τον σκοπό του πειράματος της έρευνας είναι οι εξής:

1. Foscam R2:. Η δικτυακή αυτή κάμερα έλαβε την πιστοποίηση CE της τον Σεπτέμβριο του 2018. Συνεπώς θεωρείται πως ο μήνας κυκλοφορίας της κάμερας είναι το 09/18. Άξιο αναφοράς είναι πως η κατασκευάστρια εταιρία προβαίνει σε τακτικές αναβαθμίσεις του λογισμικού της κάμερας πράγμα το οποίο προδιαθέτει πως τα προϊόντα της προβλέπεται να έχουν ψηλό επίπεδο ασφαλείας.

Εικόνα 4.1: Η δικτυακή κάμερα Foscam

2. TP-Link NC450: Το μοντέλο αυτό της εταιρίας TP-Link πήρε το CE Mark της τον Αύγουστο του 2017. Αν και κατά 1 χρόνο πιο παλιά από το μοντέλο της Foscam η συγκεκριμένη κάμερα κουβαλά στις πλάτες της ένα μεγάλο όνομα στην κατασκευή τόσο οικιακών όσο και επαγγελματικών συσκευών δικτύου. Αυτό αυξάνει τις προσδοκίες που διατηρεί ο ερευνητής όσον αφορά το επίπεδο ασφάλειας το οποίο συνοδεύει την κάμερα.

Εικόνα 4.2: Η δικτυακή κάμερα TP-Link

3. Reolink RLC 420: Αυτή η δικτυακή κάμερα από τα εγχειρίδια της δεν φαίνεται να έχει CE mark αν και είναι διαθέσιμη στην Ευρωπαϊκή αγορά. Η κάμερα κυκλοφόρησε το 2018 με ημερομηνία διάθεσης στο amazon.de τον Ιούλιο 2018. Η εταιρία φαίνεται αρκετά καινούργια στον τομέα των δικτυακών καμερών καθώς δεν υπάρχουν αρκετά στοιχεία (manuals και firmware) για τα διάφορα μοντέλα της.

Εικόνα 4.3: Η δικτυακή κάμερα TP-Link

Οι τρείς αυτές κάμερες έρχονται από 3 διαφορετικούς κατασκευαστές και έχουν διαφορετικό τρόπο λειτουργίας όπως μπορεί να φανεί από τα εγχειρίδια τους.

Τα εγχειρίδια και προδιαγραφές των καμερών επισυνάπτονται στο Παράρτημα Α.
Το κύριο μέλημα της έρευνας αποτελεί την αξιοπιστία. Συνεπώς πρώτου ξεκινήσει η οποιαδήποτε διαδικασία αξιολόγησης των ευπαθειών, των εν λόγο δικτυακών καμερών, οι κάμερες θα μπουν στην κατάσταση εργοστασιακών ρυθμίσεων, θα αναβαθμιστούν στο τελευταίο firmware το οποίο έχει εκδώσει ο εκάστοτε κατασκευαστής. Ενδεχομένως κάποιες ευπάθειες των συσκευών να έχουν αντιμετωπιστεί από τους κατασκευαστές, και στη συνέχεια θα γίνει η έναρξη του πειράματος.
Στην προκαταρκτική αξιολόγηση το πείραμα θα λάβει χώρα με τις κάμερες να έχουν μονάχα ρύθμιση δικτύου και τις ρυθμίσεις κωδικών των κατασκευαστών (πράγμα που η πλειονότητα των χρηστών δεν αλλάζει εκτός και αν τους αναγκάσει το firmware του κατασκευαστή). Καθώς ο πιο αδύνατος κρίκος στον τομέα της ασφάλειας σχεδόν όλων των πληροφοριακών συστημάτων είναι ο ανθρώπινος παράγοντας, η μη ορθή καθοδήγηση στα ζητήματα ασφαλείας κατά την αρχική ρύθμιση των συσκευών αυτών, είναι καίριο πλήγμα στην ευπάθεια των συσκευών αυτών.

4.1.3 ΚΑΤΑΓΡΑΦΕΑΣ ΔΕΔΟΜΕΝΩΝ (LOGGER).

Για τη συλλογή των δεδομένων θα χρησιμοποιηθεί ένας ηλεκτρονικός υπολογιστής με ethernet κάρτα δικτύου και λειτουργικό σύστημα Ubuntu Linux 18.10. Ο Ηλεκτρονικός αυτός υπολογιστής θα ενωθεί στο port 24 του switch στο οποίο θα γίνονται mirror οι θύρες από τις 3 κάμερες και τον επιτιθέμενο host έτσι ώστε να υπάρχει μια σφαιρική εικόνα του τι γίνεται στο δίκτυο κατά την διενέργεια μιας επίθεσης. Ο υπολογιστής αυτός δεν θα έχει ρυθμίσεις δικτύου ο ίδιος, αφού το ethernet interface του θα ενεργοποιηθεί μέσω της εντολής ip link set eth0 up και στη συνέχεια μέσω tcpdump -i eth0 θα συλλεχθούν όσα δεδομένα περνούν από την διεπαφή ethernet.

4.1.4 ΕΠΙΘΕΤΙΚΟΣ ΗΛΕΚΤΡΟΝΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ (ATTACKER).

Για τους σκοπούς του πειράματος θα χρησιμοποιηθεί και 2ος ηλεκτρονικός υπολογιστής στον ρόλο του επιτιθέμενου. Ο υπολογιστής αυτός θα τρέχει την τελευταία έκδοση του Kali Linux για σκοπούς διενέργειας δοκιμών διείσδυσης στις δικτυακές κάμερες ενώ ταυτόχρονα θα ρυθμιστεί πάνω του ο control server για το Mirai botnet σύμφωνα με τις οδηγίες του δημιουργού του οι οποίες μπορούν να βρεθούν στο Github : https://github.com/jgamblin/Mirai-Source-Code/blob/master/ForumPost.txt . Μετά την αξιολόγηση των ευπαθειών των δικτυακών

καμερών θα γίνουν απόπειρες εκμετάλλευσης από τον attacker του οποίου το command history θα καταγράφεται, ενώ τα δεδομένα δικτύου θα καταγράφονται στον Logger.

4.2 SOFTWARE REQUIREMENTS – ΑΠΑΙΤΗΣΕΙΣ ΛΟΓΙΣΜΙΚΟΥ

Το λογισμικό το οποίο προτίθεται να αξιοποιήσει η έρευνα στην προσπάθεια εύρεσης, εκμετάλλευσης και αντιμετώπισης ευπαθειών είναι το ακόλουθο συστήνεται για την υλοποίηση των πειραματικών δοκιμών είναι το ακόλουθο

4.2.1 ΑΝΑΒΑΘΜΙΣΕΙΣ FIRMWARE

Καθώς η έρευνα δεν αποσκοπεί στην ανακάλυψη παρωχημένης γνώσης θεωρείται πρέπον όπως, πριν από την έναρξης της οποιασδήποτε δοκιμής, γίνει αναβάθμιση στην τελευταία έκδοση λογισμικού της κάθε κάμερας όπως αυτό έχει εκδοθεί από την κατασκευάστρια εταιρία. Αυτό ενδέχεται να ανεβάσει την αξιοπιστία της έρευνας καθώς δεν θα αξιώνει εύσημα για ευρήματα τα οποία έχουν ήδη βρει άλλοι ερευνητές και η εταιρία έχει ήδη προσφέρει λύσεις επ' αυτών.

4.2.2 NMAP

Το nmap αποτελεί το κατ' εξοχή εργαλείο ανάλυσης δικτυακών εισόδων σε ένα στοιχείο δικτύου καθώς μπορεί να εντοπίσει ποιες δικτυακές θύρες έχει ανοικτές το στοιχείο δικτύου, το λειτουργικό του σύστημα, εκδόσεις πρωτοκόλλων τις οποίες χρησιμοποιεί και με την χρήση των ανάλογων scripts ακόμα και πιθανές ευπάθειες στις οποίες δύναται να υπόκειται το αντικείμενο υπό εξέταση. Ως εκ τούτου έχουν επιλεγει συγκεκριμένες εντολές οι οποίες θα χρησιμοποιηθούν κατά τη διάρκεια του πειράματος έτσι ώστε να συλλεχθούν οι απαραίτητες πληροφορίες που θα κατευθύνουν την έρευνα στον προσδιορισμό και αξιολόγηση των ευπαθείων στις οποίες υπόκεινται οι κάμερες. Οι εντόλές αυτές έχουν καθοριστεί ως πιο κάτω:

- sudo nmap -p 1-65535 -sV -sS -T4 < host> > <host>.txt
  Η συγκεκριμένη εντολή κάνει ολοκληρωμένο έλεγχο TCP σε όλες τις θύρες, με έλεγχο της έκδοσης της υπηρεσίας που τρέχει στο συγκεκριμένο port, ενώ χρησιμοποιεί το T4 χρονόμετρο για να στέλνει τα πακέτα προς αποφυγή εντοπισμού από τοίχος προστασίας.
- nmap -A < host> >> < host>.txt
  Η εντολή αυτή προσθέτει τον εντοπισμό του λειτουργικού συστήματος στην διαδικασία που επιτελεί το nmap ενώ περιορίζει τον έλεγχο στις γνωστές θύρες (1-1024)
- nmap -sV --version-intensity 9 < host> >> < host>.txt
  Η εντολή αυτή κάνει ένα πιο ενδελεχή έλεγχο στο αντικείμενο προς εξέταση.

- nmap -sV -sC < host> >> < host>.txt

  Η εντολή αυτή διενεργεί ένα έλεγχο χρησιμοποιώντας προκαθορισμένα ¨ασφαλή¨ scripts τα οποία ενδέχεται να μην επιφέρουν κάποια ζημιά ή εισβολή στο αντικείμενο υπό εξέταση ενώ καλύπτονται από τυχόν ανίχνευση από τοίχοι προστασίας.
- nmap -O <host> >> <host>.txt

  Καθώς το nmap -A ενδέχεται να μην αποδώσει το λειτουργικό σύστημα του αντικειμένου χρησιμοποιήθηκε και το nmap -O για να γίνει πιο ενδελεχής έλεγχος.
- nmap –script=vuln <host> >> <host>.txt

  Χρησιμοποιώντας την εντολή αυτή γίνεται μια προσπάθεια ελέγχου και αναφοράς γνωστών ευπαθειών μέσω του nmap. Η χρήση αυτής της λειτουργικότητας είναι ιδιαίτερα εύχρηστη καθώς εξοικονομεί χρόνο και ενδεχομένως να εντοπίσει αδυναμίες τις οποίες ο ερευνητής αγνοήσει.

4.2.3 BRUTUS AET2 PASSWORD CRACKER

Το εργαλείο Brutus AET2 αποτελεί ένα λογισμικό σπασίματος κωδικών το οποίο χρησιμοποιεί διάφορες μεθόδους βάση των οποίων προσπαθεί να μαντέψει τον κωδικό του χρήστη. Υποστηρίζει αρκετά πρωτόκολλα όπως http, telnet, pop3 smtp και άλλα συνεπώς μπορεί να αποβεί εξαιρετικά χρήσιμο. Μπορεί να δεχθεί 2 αρχεία, με το 1ο να είναι μια λίστα με ονόματα χρηστών ενώ το 2ο μια λίστα με πιθανούς κωδικούς. Για τους σκοπούς του πειράματος ενδέχεται να χρησιμοποιηθεί η λίστα με τους 1000 πιο διαδεδομένους κωδικούς χρηστών στο διαδίκτυο, όπως αυτοί είναι αναρτημένοι στη σελίδα του Github. Το λογισμικό αυτό έχει επίσης τη δυνατότητα να διενεργεί brute force attacks όπου του δίνεται ένα εύρος χαρακτήρων να χρησιμοποιήσει και δοκιμάζει διαφορετικούς συνδυασμούς αυτών των χαρακτήρων μέχρις ότου βρεθεί ο κωδικός. Εννοείτε πως μια τέτοια διαδικασία είναι αρκετά χρονοβόρα εξού και η επιλογή των πιο κοινών κωδικών, εφόσον και προηγούμενες έρευνες έχουν αποδείξει πως η συνήθης πρακτική των botnet είναι ο έλεγχος των πιο κοινών κωδικών. Στο παρών στάδιο υπάρχει μόνο έκδοση για Windows συνεπώς για την χρήση του θα αντικατασταθεί προσωρινά ο επιτιθέμενος υπολογιστής.

4.2.4 MIRAI BOTNET

Η έρευνα αποσκοπεί στον εντοπισμό αδυναμιών οι οποίες των οποίων η εκμετάλλευση μπορεί να αυτοματοποιηθεί, κατά συνέπεια να ενσωματωθεί σε script και να δρα σαν botnet, για να μπορέσει στο τέλος να καθορίσει ένα πλαίσιο ασφαλείας, το οποίο αν ακολουθηθεί να καθιστά τις κάμερες άτρωτες σε επιθέσεις. Στην περίπτωση που οι αρχικές δοκιμές με nmap εντοπίσουν ανοικτή την θύρα 23 την οποία χρησιμοποιεί το botnet Mirai τότε θα γίνει δοκιμή υλοποίησης και

καταγραφής της επίθεσης, προσφέροντας έτσι μια ενδελεχή ματιά στον τρόπο με τον οποίο δρα και το botnet. Ο Ηλεκτρονικός υπολογιστής ο οποίος θα δρα σαν επιτιθέμενος θα λάβει την ανάλογη ρύθμιση έτσι ώστε να καταστεί Command and Control server για το Mirai botnet το οποίο θα αφεθεί εντός του δικτύου προς παρακολούθηση και συμπεράσματα.

Κεφάλαιο 5
Υλοποίηση Πειράματος

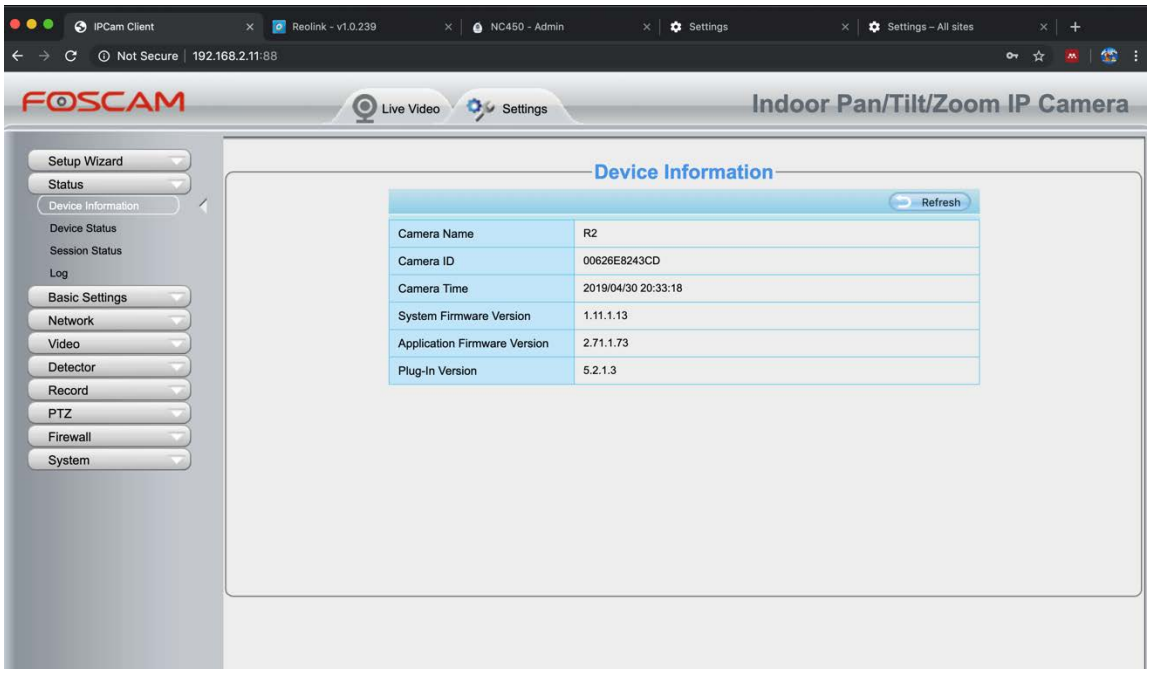
Με την ανασκόπηση της υφιστάμενης βιβλιογραφίας και ερευνών οι οποίες έχουν γίνει στον τομέα των δικτυακών καμερών, η έρευνα θα επιχειρήσει με την δική της προσέγγιση να ελέγξει την πρόοδο την οποία έχουν κάνει οι κατασκευαστές σε θέματα ασφάλειας. Ως εκ τούτου παρατίθενται πιο κάτω τα βήματα τα οποία έλαβαν χώρα κατά την διάρκεια των πειραματικών δοκιμών μαζί με τα αποτελέσματα τα οποία λήφθηκαν έτσι ώστε να μπορούν να αξιολογηθούν τόσο για τους σκοπούς αυτής της έρευνας αλλά και από μελλοντικές έρευνες οι οποίες μπορούν να προκύψουν από τα ευρήματα.

5.1 ΑΝΑΒΑΘΜΙΣΗ FIRMWARE.

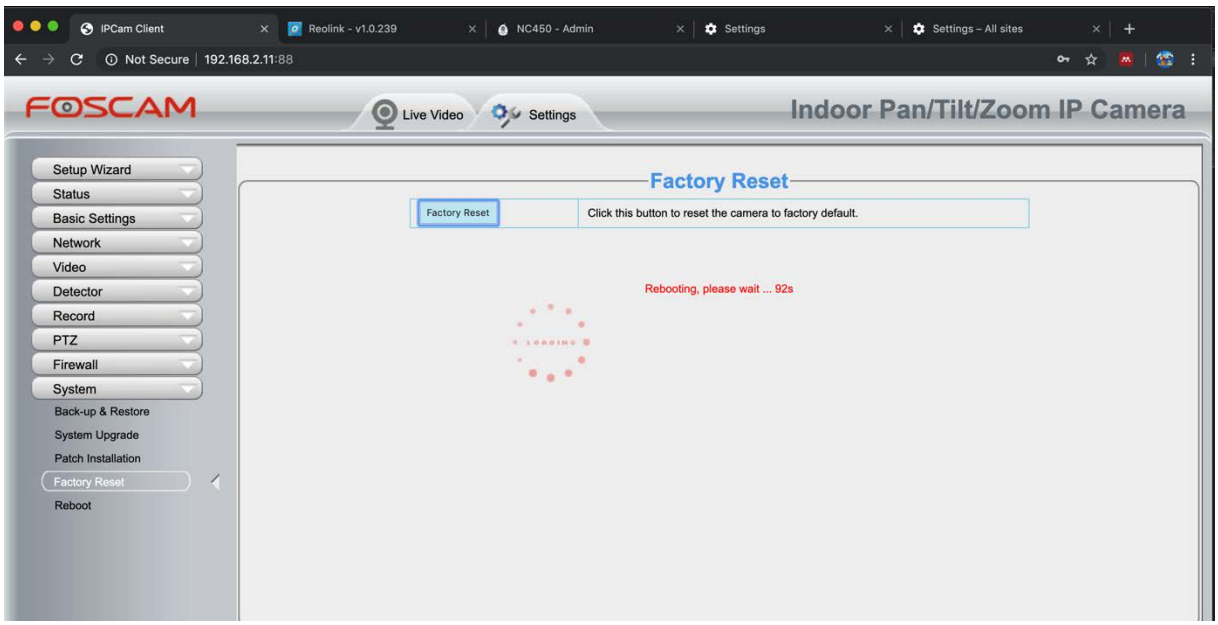
Για την σωστή αξιολόγηση του παρόντος επιπέδου ασφαλείας των δικτυακών καμερών θεωρείται σωστό όπως το λογισμικό των καμερών είναι αναβαθμισμένο στην τελευταία έκδοση την οποία έχει διαθέσιμη ο εκάστοτε κατασκευαστής. Αυτό θα βοηθήσει στην εξακρίβωση των μέτρων ασφαλείας και τον βαθμό τον οποίο έχουν ληφθεί, στις πιθανές ελλείψεις όπως επίσης και στην πρόταση επιπρόσθετων μέτρων τα οποία να θωρακίζουν περαιτέρω την ασφάλεια των δικτυακών καμερών τόσο από botnets αλλά και από άλλους κινδύνους γενικότερα.

5.1.1 FOSCAM R2.

Το τελευταίο firmware που έχει εκδώσει ο κατασκευαστής Foscam για το συγκεκριμένο μοντέλο κυκλοφόρησε στις 17/04/2019, και θα εγκατασταθεί άμεσα στην υπό εξέταση κάμερα. Αν και δεν δίνονται πολλές πληροφορίες στο αρχείο αναφοράς (changelog) σχετικά με την αναβάθμιση, εκθειάζονται κάποιες βελτιώσεις στην λειτουργία της κάμερας χωρίς όμως να γίνεται αναφορά σε κάποιο θέμα ασφάλειας. Μετά την διαδικασία αναβάθμισης του λογισμικού επιβεβαιώνεται ότι τρέχει η νεότερη έκδοση και στη συνέχεια η κάμερα ρυθμίζεται να επιστρέψει στις εργοστασιακές της ρυθμίσεις:



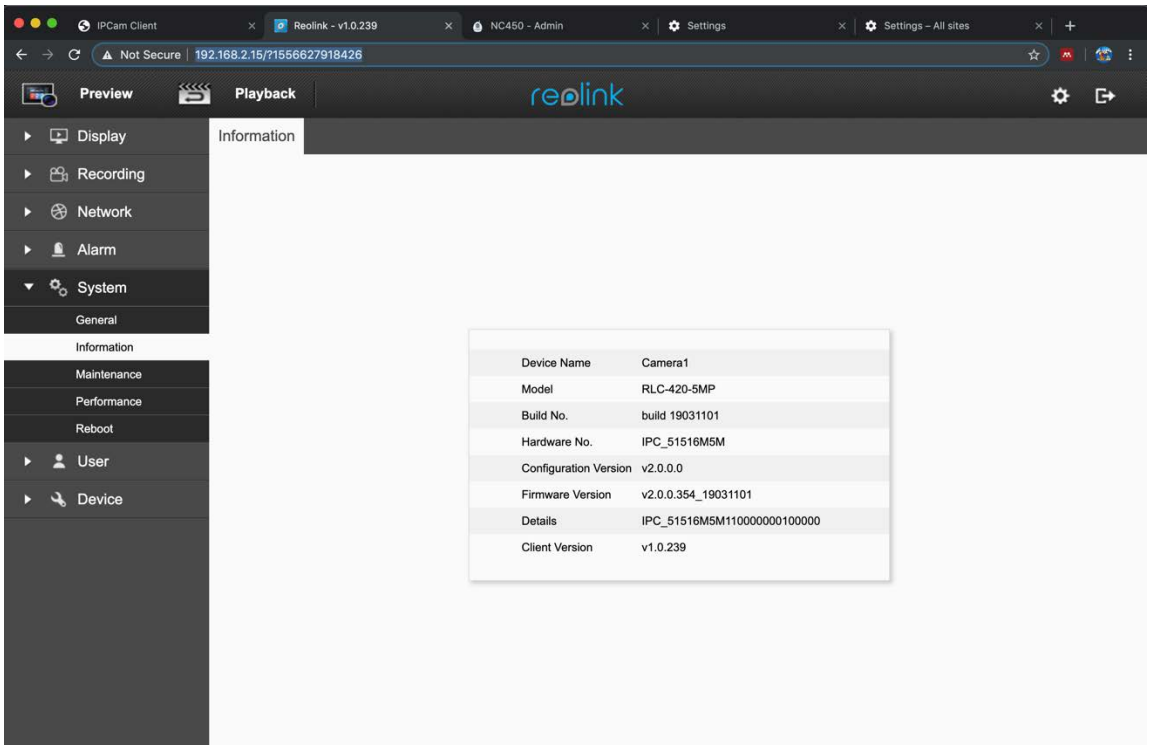
Εικόνα 5.1: Το Αναβαθμισμένο λειτουργικό της κάμερας Foscam



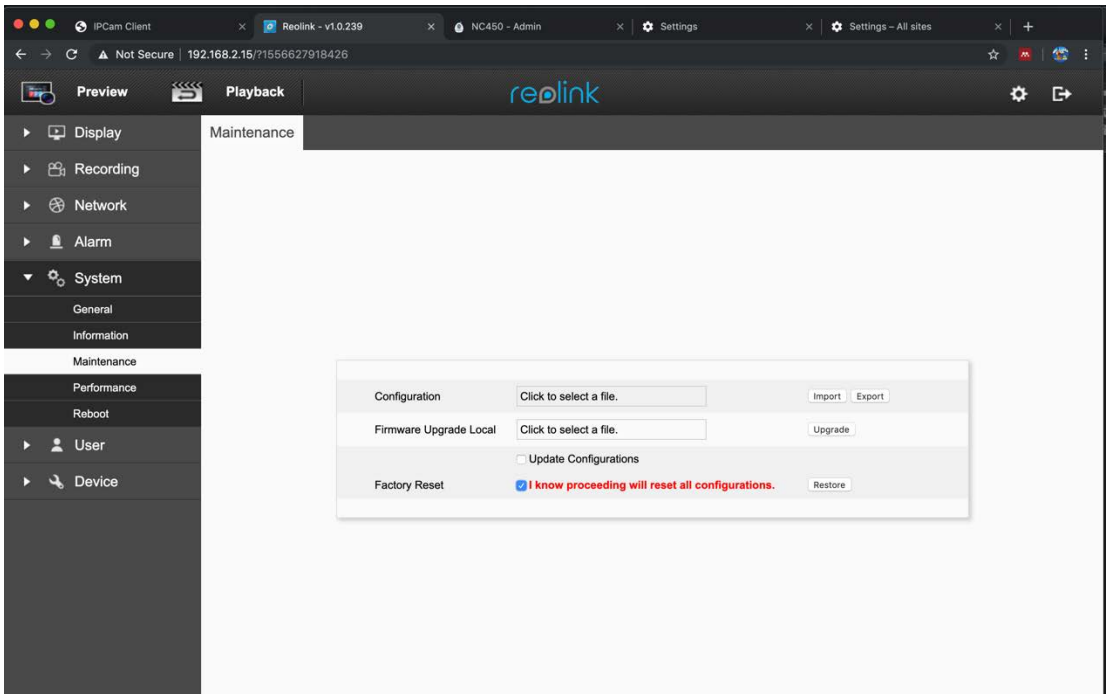
Εικόνα 5.2: Επαναφορά των εργοστασιακών ρυθμίσεων στην κάμερα Foscam

5.1.2 REOLINK RLC-420-5MP

Η εταιρία Reolink επίσης κυκλοφόρησε την τελευταία έκδοση firmware, για το εν λόγο μοντέλο, αρκετά πρόσφατα, με ημερομηνία έκδοσης 11/03/19. Το αρχείο αναφοράς σχετικά με τις αλλαγές / προσθήκες στο συγκεκριμένο firmware δεν κάνουν αναφορά σε θέματα ασφαλείας της κάμερας και περιορίζονται στις διάφορες λύσεις μικροπροβλημάτων (bug fixes) στις οποίες υπόκειντο η κάμερα. Μετά την αναβάθμιση η κάμερα ρυθμίστηκε στις εργοστασιακές της ρυθμίσεις ως προετοιμασία των πειραματικών δοκιμών.



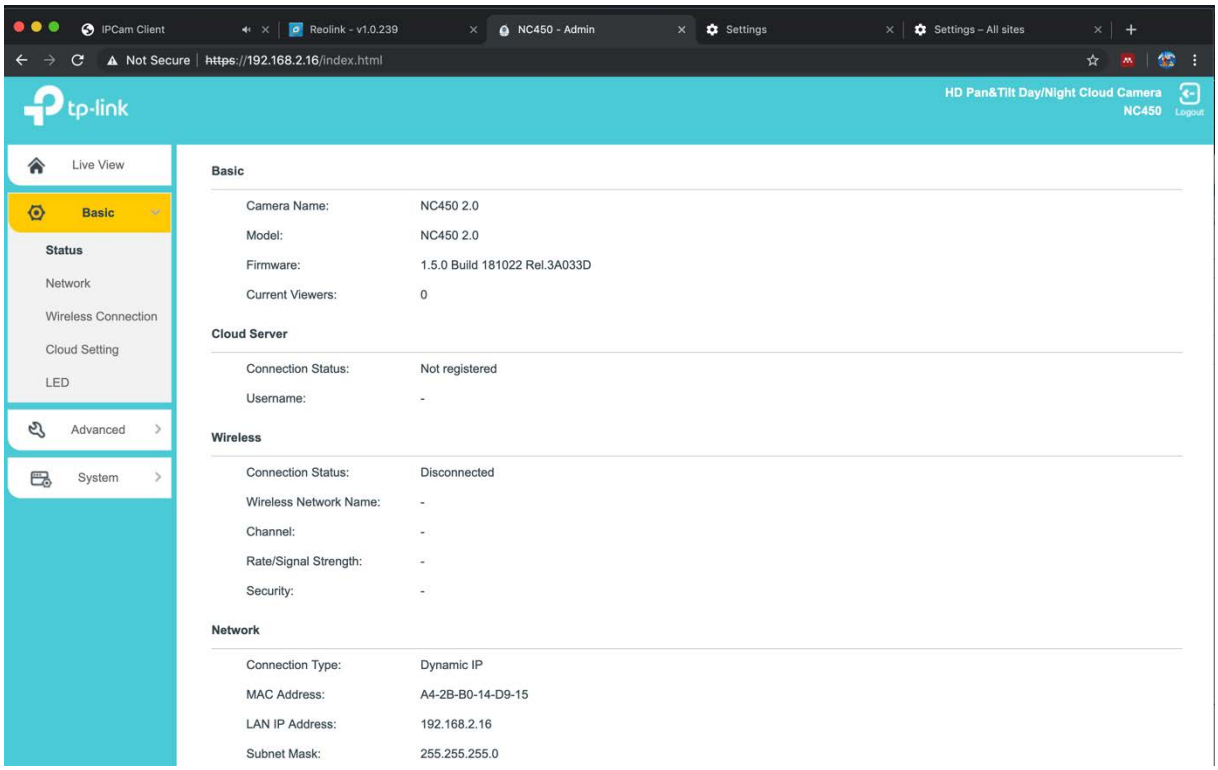
Εικόνα 5.3: Το Αναβαθμισμένο λειτουργικό της κάμερας Reolink



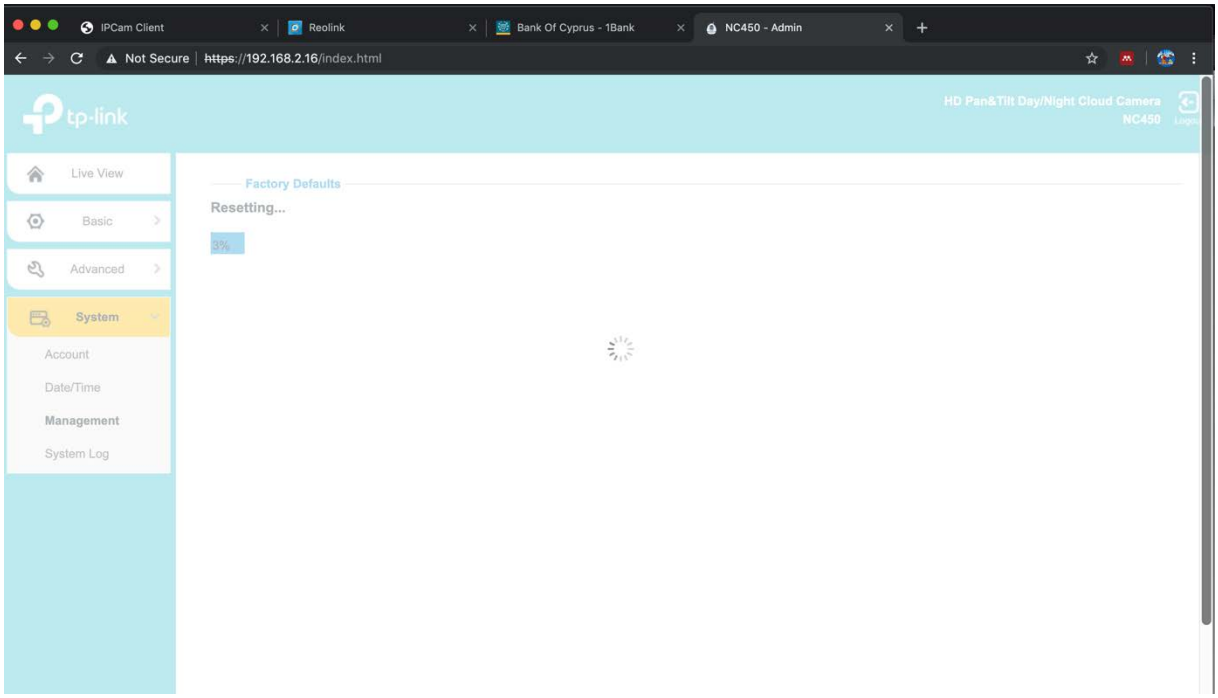
Εικόνα 5.4: Επαναφορά των εργοστασιακών ρυθμίσεων στην κάμερα Reolink

5.1.3 TP-LINK NC450 2.0

Στην περίπτωση της κάμερας TP-Link παρατηρούμε πως το λογισμικό είναι αρκετά πιο παλαιό καθώς η εταιρία έκδωσε για τελευταία φορά firmware update στις 17/12/2018 με το αρχείο αναφοράς να αναφέρει υποστήριξη HTML5 για περισσότερους φυλλομετρητές όπως επίσης και βελτίωση στην ασφάλεια αποστολής δεδομένων, χωρίς όμως να προβαίνει σε λεπτομέρειες ώς προς τί είναι αυτή η βελτίωση. Όπως και στις προηγούμενες κάμερες μετά την αναβάθμιση και την επιβεβαίωση της, η κάμερα επιστρέφεται στις εργοστασιακές της ρυθμίσεις για την συνέχεια του πειράματος.



Εικόνα 5.5: Το Αναβαθμισμένο λειτουργικό της κάμερας TP-Link



Εικόνα 5.6: Επαναφορά των εργοστασιακών ρυθμίσεων της κάμερας TP-Link

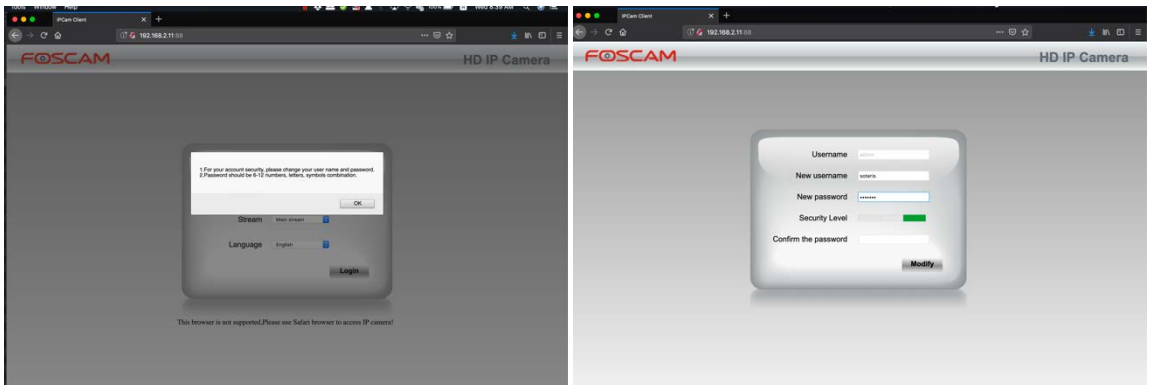
5.2 ΑΡΧΙΚΟΠΟΙΗΣΗ ΚΑΜΕΡΩΝ.

Το πρώτο βήμα μετά την αναβάθμιση του λογισμικού και επαναφορά των καμερών στις εργοστασιακές τους ρυθμίσεις, είναι η ρύθμιση καμερών με όσον το δυνατό λιγότερο παρεμβατικό τρόπο ώστε να καταστούν οι κάμερες λειτουργικές. Ο σκοπός είναι να ακολουθηθούν τα βήματα που απαιτεί το λογισμικό του κατασκευαστή για να μπορεί να χρησιμοποιηθεί η κάμερα. Οι ρυθμίσεις αυτές αποτελούν συνήθως τις ρυθμίσεις του ασύρματου δικτύου και διεύθυνση IP . Στην περίπτωση που ζητηθεί θα γίνει και αλλαγή του κωδικού με έλεγχο κατά πόσο η διαδικασία μπορεί να τύχει αναχαίτισης.

5.2.1 FOSCAM R2.

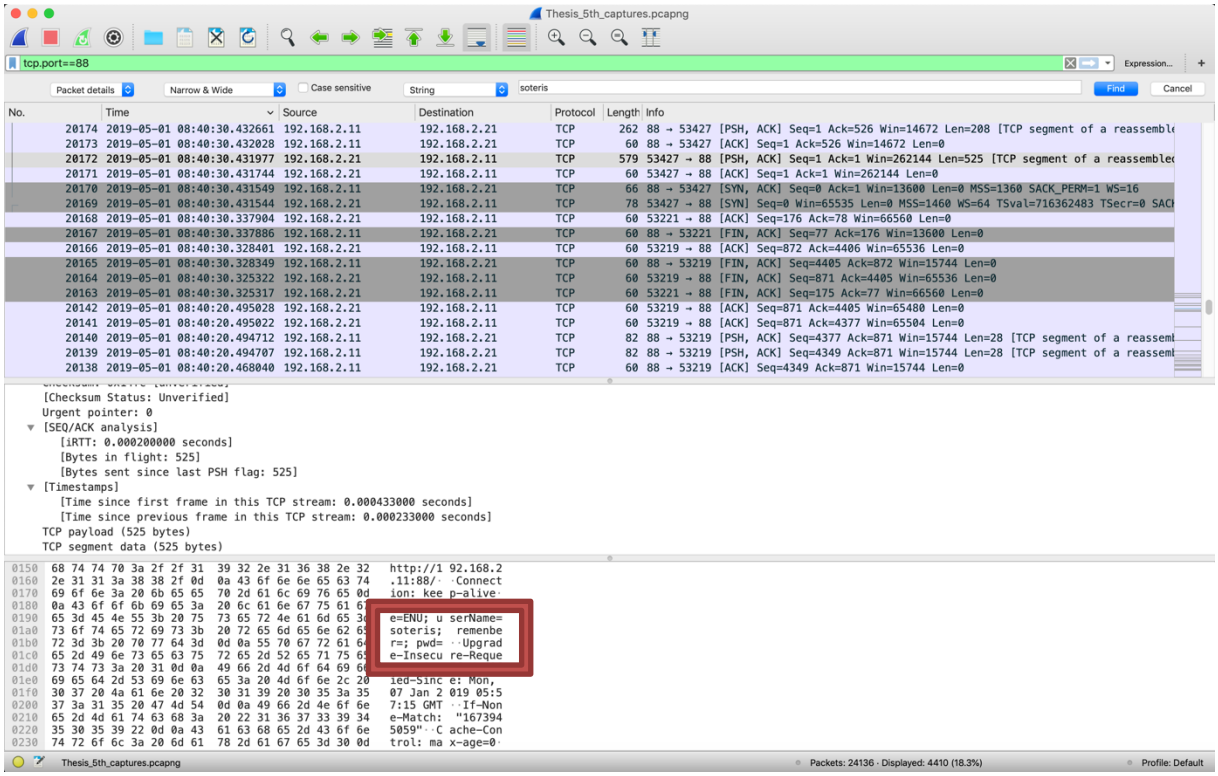
Η εργοστασιακή ρύθμιση της κάμερας αυτής δέχεται HTTP requests στην θύρα 88 αντί της θύρας 80, ενδεχομένως για να ελαχιστοποιεί τους κινδύνους που εγκυμονεί η θύρα 80, βάση της οποίας υποδεικνύεται πως η επικοινωνία που λαμβάνει χώρα δεν είναι κρυπτογραφημένη. Αν και υπάρχει και υποστήριξη στη θύρα 443 το πιστοποιητικό SSL της κάμερας δεν είναι εμπιστεύσιμο από τον φυλλομετρητή, που ελλοχεύει τον κίνδυνο επίθεσης Man in the Middle. Επίσης στην προσπάθεια ταυτοποίησης του χρήστη με ένωση στη θύρα 443 η κάμερα έδινε μήνυμα λάθους πως δεν υποστηρίζει την ταυτοποίηση χρηστών σε ενώσεις με SSL. Συνεπώς αυτό καθιστά ένα bug το οποίο θα πρέπει να επιλύσει ο κατασκευαστής.

Προτού καν ενωθεί ο χρήστης για πρώτη φορά η κάμερα ζητά από τον χρήστη την εγκατάσταση ενός plugin στον φυλλομετρητή. . Με την πρώτη ταυτοποίηση στην κάμερα χρησιμοποιώντας το αρχικό όνομα χρήστη και κωδικό (admin και κενός κωδικός) η κάμερα ζητά την αλλαγή τόσο του ονόματος χρήστη όσο και του κωδικού πρόσβασης με ένδειξη κατά πόσο ο κωδικός δυνατός ή εύκολα προβλέψιμος.



Εικόνες 5.6, 5.7: Αρχικοποίηση της κάμερας Foscam με τη σελίδα αλλαγής διαπιστευτηρίων

Η πρακτική αυτή αν και αυξάνει το επίπεδο της ασφάλειας αρκετά. Ενδεχομένως το plugin που ζητά η ιστοσελίδα να εγκατασταθεί στον υπολογιστή να κρυπτογραφεί τη διαδικασία ταυτοποίησης καθώς τα πακέτα τα οποία λήφθηκαν δεν αποκαλύπτουν τον κωδικό που τοποθετήθηκε:

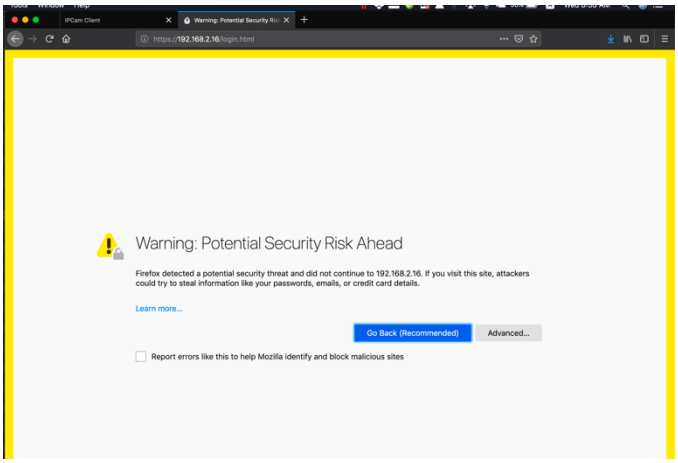


Εικόνα 5.8: Δεδομένα στο δίκτυο κατά την διάρκεια της Αυθεντικοποίησης

Το σύστημα στη συνέχεια ζητά κάποιες βασικές ρυθμίσεις σχετικά με την χώρα διαμονής / ώρα, πληροφορίες για τυχόν ασύρματα δίκτυα για τα οποία αξίζει να παρατηρηθεί πως και πάλι δε βρέθηκε ο κωδικός σε μορφή κειμένου κατά την διάρκεια της επικοινωνίας. Στη συνέχεια γίνεται μια παρέμβαση στις ρυθμίσεις IP για να αποκοπεί η σύνδεση της κάμερας με το διαδίκτυο (βάζοντας λάθος διεύθυνση router) προς αποφυγή μόλυνσης του περιβάλλοντος του πειράματος.

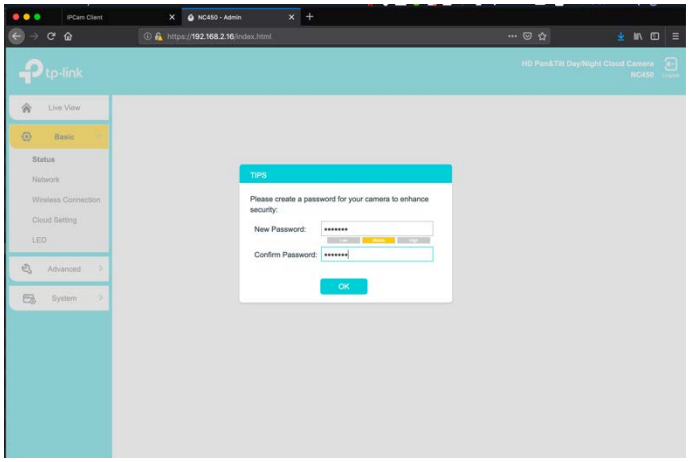
5.2.2 TP-LINK NC 450.

Στη συνέχεια η διαδικασία συνεχίστηκε στην κάμερα TP-Link της οποίας όμως η πρόσβαση στη θύρα 80 για HTTP μεταφέρεται αυτόματα στη θύρα 443 για σύνδεση HTTPS. Καθώς το πιστοποιητικό της κάμερας δεν είναι ευρέως εμπιστεύσιμο πρέπει να γίνει εξαίρεση στον φυλλομετρητή για να μπορεί να γίνει ένωση με την κάμερα:



Εικόνα 5.9: Αρχικοποίηση της κάμερας TP-Link – Προσθήκη εμπιστοσύνης πιστοποιητικού ασφαλείας.

Με τη χρήση των εργοστασιακών διαπιστευτηρίων γίνεται ένωση στη κάμερα η οποία χρειάζεται να αλλάξει ο κωδικός της προτού δεχθεί περαιτέρω ρυθμίσεις. Γίνεται η παρατήρηση πως ενώ χρησιμοποιήθηκε ο ίδιος κωδικός με την Foscam η πρώτη θεώρησε τον κωδικό σαν δυνατό ενώ η TP-Link τον κατατάσσει σαν μέτριας δύναμης:



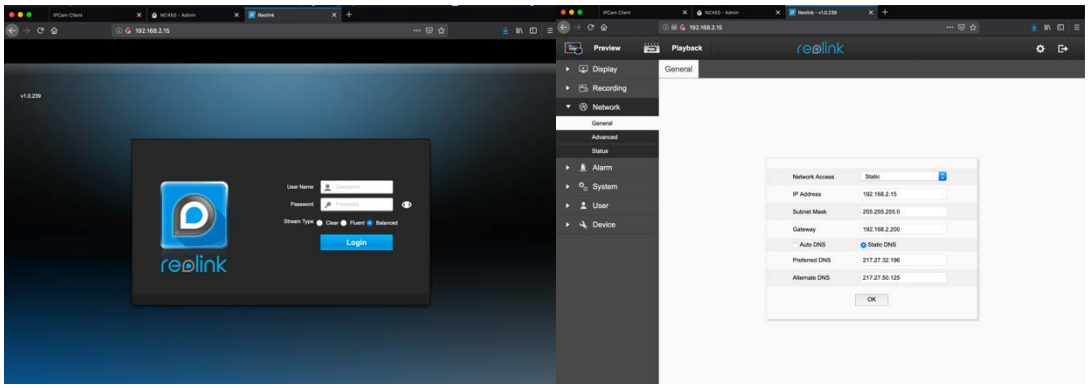
Εικόνα 5.10 : Αλλαγή κωδικού χρήστη στην κάμερα TP-Link.

Στην περίπτωση της TP-Link δεν απαιτήθηκαν άλλες ρυθμίσεις συνεπώς αλλάχθηκε μόνο η ρύθμιση IP για να αποκοπεί η σύνδεση της κάμερας με το διαδίκτυο. Με την χρήση του

πιστοποιητικού SSL όλη η επικοινωνία ήταν κρυπτογραφημένη και δεν έγινε η αναγνώριση κάποιου πακέτου.

5.2.3 REOLINK RLC-420-5MP.

Εκ πρώτης όψεως η κάμερα αυτή δέχεται ενώσεις HTTP στη θύρα 80 ενώ το λογισμικό της δεν εξαναγκάζει την αλλαγή του εργοστασιακού κωδικού της. Καθώς έχει ήδη αποφασιστεί πως δεν θα γίνει καμία απολύτως ρύθμιση πέραν αυτών που χρειάζεται το λογισμικό για να λειτουργήσει, και την αποκοπή από το διαδίκτυο, ο ερευνητής προχωρά μόνο στις ρυθμίσεις IP:



Εικόνες 5.11, 5.12: Αρχικοποίηση της κάμερας Foscam με τη σελίδα αλλαγής διαπιστευτηρίων

Καθώς η κάμερα δεν προσφέρει κάποια προκαθορισμένη κρυπτογράφηση και ο κωδικός της κάμερας παραμένει κενός αναμένεται πως το επίπεδο ασφάλειας της κάμερας δεν θα είναι τόσο ψηλό. Η κάμερα δεν υποστηρίζει ασύρματες ενώσεις συνεπώς δεν ερευνήθηκε το ενδεχόμενο υποκλοπής του ασύρματου δικτύου και του κωδικού του.

5.2.4 ΣΧΟΛΙΑ – ΓΕΝΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Καθώς ένα botnet μπορεί να απευθύνεται σε πολύ συγκεκριμένο κοινό, μια συγκεκριμένη μάρκα ή ακόμα ένα συγκεκριμένο μοντέλο εξοπλισμού, η έρευνα θεωρεί ιδιαίτερα σημαντική την μελέτη ποικιλίας κατασκευαστών. Όπως παρατηρήθηκε κατά την αρχικοποίηση των καμερών υπάρχουν διαφορετικές προσεγγίσεις ως προς τα μέτρα και τα επίπεδα ασφάλειας που εφαρμόζει ο κάθε κατασκευαστής στα προϊόντα του. Αυτό έχει να κάνει με την έλλειψη όπως προαναφέρθηκε κάποιου κοινού πρωτοκόλλου, ή έστω μίας κοινής οδηγίας, σε θέματα ασφάλειας, το οποίο να αναγκάζει και να ωθεί τους κατασκευαστές στην ασφάλεια by default. Οι κατασκευαστές Foscam και TP-Link σε αυτό το βήμα αν και κινούνται στη σωστή κατεύθυνση εν τούτοις παρουσιάζουν ελλείψεις στο θέμα της κρυπτογραφίας καθώς το πιστοποιητικό το οποίο χρησιμοποιείται δεν είναι έμπιστο. Επίσης θα μπορούσαν να παρείχαν οδηγίες κατά την διαδικασία αλλαγής του κωδικού που να καθοδηγούσαν τον χρήστη στην κατασκευή ενός

δυνατού κωδικού. Όσον αφορά την εταιρία Reolink σε αυτή την φάση είναι εμφανές πως υπάρχει παντελής έλλειψη σε θέματα ασφάλειας.

5.3 ΑΝΙΧΝΕΥΣΗ ΘΥΡΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ (NMAP).

Στη διαδικασία εντοπισμού της οποιασδήποτε αδυναμίας σε ένα πληροφοριακό σύστημα, η νευραλγική διαδικασία είναι ο εντοπισμός των υπηρεσιών που παρέχει το πληροφοριακό σύστημα. Αυτό κατ' επέκταση θα αποκαλύψει τις θύρες οι οποίες είναι ανοικτές. Στη συνέχεια η διαπίστωση του λειτουργικού συστήματος και οι εκδόσεις των λογισμικών οι οποίες παρέχουν τις εν λόγο υπηρεσίες, αρχίζουν να ζωγραφίζουν την εικόνα σχετικά με το πως πρέπει να σχεδιαστεί μια επίδοξη επίθεση στο σύστημα αυτό. Το λογισμικό το οποίο μπορεί να παράσχει τις πληροφορίες αυτές είναι το nmap ή zenmap, στην περίπτωση που επιθυμείται ένα γραφικό περιβάλλον, και είναι διαθέσιμο σε Linux, Windows και macOS. Έχοντας αναλύσει την σημασία που έχει η εύρεση των υπηρεσιών και θυρών τις οποίες προσφέρει ένα υπολογιστικό σύστημα, όπως μια δικτυακή κάμερα. Η έρευνα στη συνέχεια θα εξετάσει τις 3 κάμερες του πειράματος αφενός για να ελέγξει τις υπηρεσίες οι οποίες τρέχουν και αφετέρου να προσπαθήσει να εντοπίσει τυχόν ευπάθειες οι οποίες μπορεί να υπάρχουν. Εάν υπάρχουν κοινές ευπάθειες οι οποίες ενδεχομένως να δίνουν root πρόσβαση στις κάμερες μπορούν να θεωρηθούν Πρόδρομοι για την ανάπτυξη του αντίστοιχου botnet. Το λογισμικό αυτό έχει χρησιμοποιηθεί στην έρευνα αυτή με τα εξής αποτελέσματα.

5.3.1 FOSCAM R2.

Κατά την δοκιμή της κάμερας με το nmap βρέθηκαν οι πιο κάτω υπηρεσίες και θύρες στη κάμερα:

Θύρα	Κατάσταση	Υπηρεσία	Έκδοση Λογισμικού
88	Ανοικτή	HTTP	lighttpd
443	Ανοικτή	HTTPS	lighttpd
888	Ανοικτή	gsoap / Onvif	gSOAP
65534	Ανοικτή	rtsp	rtsp

Πινακας 5.1: Υπηρεσίες και ανοικτές θύρες στη κάμερα Foscam.

Το ολοκληρωμένο αρχείο που έχει τα αποτελέσματα όλων των εντολών επισυνάπτεται στο Παράρτημα Α. Αν και σε καμιά περίπτωση δεν αναφέρονται οι εκδόσεις του lighttpd το λειτουργικό σύστημα πολύ σωστά υποδεικνύεται σαν webcam με μία επιπρόσθετη πληροφορία σχετικά με το υλισμικό της κάμερας το οποίο είναι: cpe:/h:pelco:ide10dn. Σχετικό ψάξιμο στο διαδίκτυο συνδέει τον συγκεκριμένο τύπο κάμερας με την εταιρία κατασκευής Pelco και πιο συγκεκριμένα με τις κάμερες της γραμμής Spectra IV IP. Η πληροφορία αυτή μπορεί να αποδειχθεί ιδιαίτερα χρήσιμη καθώς τυχόν ευπάθεια που επηρεάζει το συγκεκριμένο μοντέλο κάμερας

ενδέχεται να επηρεάσει και την άλλη μάρκα αυξάνοντας έτσι το πλήθος των ευάλωτων συσκευών. Οι πιθανές ευπάθειες οι οποίες έχουν εντοπιστεί από το nmap και τις πληροφορίες οι οποιες προέκυψαν από την ανάλυση την οποίες έκανε παρατίθενται στον πιο κάτω πίνακα:

Α/Α	**Αρ. CVE**	**Επικυνδινότητα**	**Περιγραφή**	**Εφαρμόσιμο σε botnet**
1	CVE-2014-3704	6.4	Η ευπάθεια αυτή επιτρέπει σε επιτιθέμενους να πραγματοποιήσουν επιθέσεις SQL Injection καθώς το Drupal API δεν δημιουργεί ορθά τα SQL statements . Η ευπάθεια αυτή δεν δίνει πρόσβαση στη κάμερα συνεπώς δεν καθιστά χρήση σε botnet.	Αρνητικό
2	CVE-2019-11072	7.5	Η ευπάθεια αυτή καθιστά τον webserver lighttp τον οποίο χρησιμοποιεί η συγκεκριμένη κάμερα ευάλωτο σε επίθεση signed integer overflow. Η επίθεση αυτή μπορεί να προξενήσει Denial of Service αλλά δεν δίνει πρόσβαση στην κάμερα, συνεπώς δεν καθιστά κίνδυνο υλοποίηση σε botnet	Αρνητικό
3	CVE-2017-9765	8.6	Η συγκεκριμένη ευπάθεια απευθύνεται στο πρωτόκολλο ONVIF το οποίο χρησιμοποιείται για να δώσει τη δυνατότητα σε NVR συσκευές να ενώνονται σε κάμερες από διαφορετικούς κατασκευαστές. Βασίζεται στην εκμετάλλευση του gSOAP. Μπορεί να χρησιμοποιηθεί για την εκτέλεση εντολών, αλλαγή ρυθμίσεων και λειτουργίας της κάμερας και ενδεχομένως να μπορεί να κωδικοποιηθεί σε botnet.	Θετικό

Πινακας 5.2: Ευπάθειες στη κάμερα Foscam.

Εδώ αξίζει να σημειώσουμε πως το γεγονός ότι η κάμερα χρησιμοποιεί την θύρα 88 για την εξυπηρέτηση της υπηρεσίας HTTP κατά κάποιο τρόπο καθιστά τους αυτόματους ελέγχους για ευπάθειες ολίγο παρωχημένους καθώς αυτοί κοιτάζουν συγκεκριμένα την θύρα 80. Αυτό δεν καθιστά την κάμερα άτρωτη σε επίθεση, αλλά την κάνει σίγουρα πιο διακριτική σε τυχόν αυτόματες ανιχνεύσεις.

5.3.2 TP-LINK NC450.

Τα ευρήματα της δοκιμής στην δεύτερη κάμερα της έρευνας, της TP-Link NC450, παρατίθενται στον πιο κάτω πίνακα:

Θύρα	Κατάσταση	Υπηρεσία	Έκδοση Λογισμικού
80	Ανοικτή	HTTP	Lighttpd 1.4.32
443	Ανοικτή	HTTPS	Lighttpd 1.4.32
554	Ανοικτή	rtsp	DoorBird Video Doorbell rtspd
2020	Ανοικτή	Soap	gSoap 2.8
8080	Ανοικτή	http-proxy	Streamd, A42BB014D915
8081	Ανοικτή	Blackice-icecap	
8088	Ανοικτή	Radan-http	vod

Πινακας 5.3: Υπηρεσίες και ανοικτές θύρες στη κάμερα TP-Link.

Το ολοκληρωμένο αρχείο με τα αποτελέσματα των εντολών έχουν προστεθεί στο παράρτημα Α. Το λειτουργικό σύστημα της κάμερας αυτής έχει εντοπιστεί να είναι η έκδοση Kamikaze του Openwrt με έκδοση Linux kernel 2.6.26. Η πληροφορία αυτή θα μας δώσει ενδείξεις για πιθανές ευπάθειες οι οποίες μπορεί να σχετίζονται με αυτή την έκδοση λειτουργικού συστήματος. Με βάση τις πληροφορίες, οι οποίες συλλέχθηκαν με την χρήση της εντολής nmap γίνεται εκ νέου έρευνα στο διαδίκτυο έτσι ώστε να εντοπιστούν οι ευπάθειες οι οποίες πιθανώς να επηρεάζουν την συγκεκριμένη συσκευή. Στον πιο κάτω πίνακα παρατίθενται οι ευπάθειες οι οποίες βρέθηκαν από το nmap αλλά κι από τις εκδόσεις λογισμικού που είναι εγκατεστημένες στην κάμερα:

Α/Α	**Αρ. CVE**	**Επικυνδινότητα**	**Περιγραφή**	**Εφαρμόσιμο σε botnet**
1	CVE-2007-6750	5	Η ευπάθεια αυτή κάνει το σύστημα τρωτό σε επιθέσεις Denial of Service καθώς δεν υπάρχει καθορισμένο timeout στα http requests. Δεν παρέχεται πρόσβαση στο σύστημα συνεπώς δεν μπορεί να εφαρμοστεί σε botnet	Αρνητικό
2	CVE-2014-3566	6.8	Η χρήση του SSL3.0 στο OpenSSL δεν χρησιμοποιεί καθοριστικό CBC padding κάνοντας το ευάλωτο σε Man in the Middle Attack. Καθώς η διαδικασία δεν μπορεί να αυτοματοποιηθεί δεν καθιστά κίνδυνο χρήσης σε botnet.	Αρνητικό

3	CVE-2018-19630	4.3	Η ευπάθεια αυτή προκύπτει από το λειτουργικό σύστημα, καθώς δεν γίνεται απόκρυψη του path σε ορισμένα http requests κάνοντας το σύστημα ευαίσθητο σε παραποίηση αρχείων. Δεν μπορεί να κωδικοποιηθεί σε botnet	Αρνητικό
4	CVE-2018-11116	6.5	Λάθος διαχείριση του /etc/config/rcpd από το λειτουργικό σύστημα μπορεί να επιτρέψει σε επικυρωμένους χρήστες να καλέσουν μεθόδους και λειτουργίες για τις οποίες δεν έχουν πρόσβαση. Η ευπάθεια αυτή μπορεί να κωδικοποιηθεί σε botnet στην περίπτωση που δεν γίνει χρήση ισχυρού κωδικού κατά την αρχικοποίηση της κάμερας.	Θετικό
5	CVE-2014-2324	5	Η ευπάθεια αυτή μπορεί να δώσει πρόσβαση σε χρήστες να διαβάσουν αρχεία στα οποία δεν έχουν πρόσβαση. Δεν υπάρχει κίνδυνος χρήσης σε botnet	Αρνητικό
6	CVE-2014-2323	7.5	Υπάρχει κίνδυνος για SQL Injection attack καθώς ο web server δεν χειρίζεται σωστά κάποιά κάποια functions. Η ευπάθεια αυτή δεν επηρεάζει την κάμερα καθ΄αυτό καθώς δεν συνδέεται με βάση δεδομένων. Δεν υπάρχει κίνδυνος χρήσης σε botnet	Αρνητικό
7	CVE-2013-4560	2.6	Ο Web Server είναι ευπαθής σε segmentation fault που μπορει να τύχει εκμετάλλευσης και να προξενήσει DoS. Δεν υφίσταται κίνδυνος χρήσης σε botnet	Αρνητικό
8	CVE-2013-4559	7.6	Αυτή η έκδοση του lighttp δεν ελέγχει τα πεδία setuid, setgid και setgrpoups που δίνει την δυνατότητα στον επιτιθέμενο να επανεκκινήσει τον web server με δικαιώματα root και να παράσχει πρόσβαση.	Θετικό
9	CVE-2017-9765	8.6	Η συγκεκριμένη ευπάθεια απευθύνεται στο πρωτόκολλο ONVIF το οποίο χρησιμοποιείται για να δώσει τη δυνατότητα σε NVR συσκευές να ενώνονται σε κάμερες από διαφορετικούς κατασκευαστές. Βασίζεται στην εκμετάλλευση του gSOAP. Μπορεί να χρησιμοποιηθεί για την εκτέλεση εντολών, αλλαγή ρυθμίσεων και λειτουργίας της κάμερας ενδεχομένως να μπορεί να κωδικοποιηθεί σε botnet.	Θετικό

Πινακας 5.4: Ευπάθειες που εντοπίστηκαν στη κάμερα TP-Link.

5.3.3 REOLINK RLC-420-5MP.

Από τα αρχικά στάδια η κάμερα αυτή θα μπορούσε να θεωρηθεί η πιο επιρρεπής σε ευπάθειες και αδυναμίες καθώς δεν πρόσφερε προεπιλεγμένα κρυπτογραφική επικοινωνία αλλά ούτε και ανάγκαζε τον χρήστη να θέσει ή να αλλάξει τον προεπιλεγμένα απών κωδικό της. Με την χρήση του nmap βρέθηκαν οι πιο κάτω υπηρεσίες να τρέχουν με τις ανάλογα ανοικτές θύρες όπως καταγράφονται στον πίνακα:

Θύρα	Κατάσταση	Υπηρεσία	Έκδοση Λογισμικού
80	Ανοικτή	HTTP	nginx 1.6.2
443	Ανοικτή	HTTPS	nginx 1.6.2
554	Ανοικτή	rtsp	D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
1935	Ανοικτή	Rtmp	
6001	Ανοικτή	Rtsp	D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
8000	Ανοικτή	onVIF	gSOAP2.8
9000	Ανοικτή	Cslistener	
17823	Open	http	nginx 1.6.2

Πινακας 5.5: Υπηρεσίες και ανοικτές θύρες στη κάμερα Reolink.

Όπως και η κάμερα της εταιρίας Foscam έτσι και αυτή στο πεδίο του λειτουργικού συστήματος της αναφέρει webcam και δίνει το ίδιο μοντέλο υλισμικού cpe:/h:pelco:ide10dn. Παρατηρούμε όμως πως έχουν διαφορετικές προσεγγίσεις στην προσφορά των υπηρεσιών τους αλλά και του τρόπου λειτουργίας τους. Στον πιο κάτω πίνακα παρατίθενται οι πληροφορίες σχετικά με τις ευπάθειες στις οποίες υπόκειται το συγκεκριμένο μοντέλο κάμερας. Σημείωση πως όπως και στις προηγούμενες δοκιμές οι πληροφορίες αυτές βασίζονται στο λειτουργικό σύστημα και τις εκδόσεις λογισμικών οι οποίες ανιχνεύθηκαν στην κάμερα:

Α/Α	**Αρ. CVE**	**Επικυνδινότητα**	**Περιγραφή**	**Εφαρμόσιμο σε botnet**
1	CVE-2011-3192	7.8	Η ευπάθεια αυτή επηρεάζει τον web-server της κάμερας ευάλωτο επιτρέποντας στον επιτιθέμενο να προκαλέσει DoS με την χρήση ενός Range header. Δεν καθιστά επικινδυνότητα για χρήση σε botnet	Αρνητικό

2	CVE-2014-3566	6.8	Η χρήση του SSL3.0 στο OpenSSL δεν χρησιμοποιεί καθοριστικο CBC padding κάνοντας το ευάλωτο σε Man in the Middle Attack. Καθώς η διαδικασία δεν μπορεί να αυτοματοποιηθεί δεν καθιστα κίνδυνο χρήσης σε botnet.	Αρνητικό
3	CVE-2005-3299	5	Η ευπάθεια στη php επιτρέπει την τοποθέτηση τοπικών αρχείων μέσω της $__redirect_parameter . Δεν καθιστά κίνδυνο χρήσης σε botnet αλλά περισσότερο παραποίησης των στοιχείων της κάμερας.	Αρνητικό
4	CVE-2018-16844	3.6	Η ευπάθεια αυτή μπορεί να οδηγήσει σε αυξημένη χρήση του επεξεργαστή, ένεκα λάθους υλοποίησης του http2.	Αρνητικό
5	CVE-2016-1247	7.8	Η ευπάθεια αυτή επιτρέπει σε ενωμένους χρήστες να αποκτήσουν πρόσβαση root μέσω μιας symlink επίθεσης στο error.log. Αν και ο χρήστης πρέπει να είναι ήδη ταυτοποιημένος στην κάμερα η απουσία εξαναγκασμου σε πολύπλοκο κωδικό μπορεί να επιτρέψει την πρόσβαση και να χρησιμοποιηθεί σε botnet	Θετικό
6	CVE-2016-0746	3.4	Η ευπάθεια αυτή κάνει τον web server τρωτό σε DoS μετά από μιας ειδικά κατασκευασμένης απάντησης DNS που σχετίζεται με CNAME processing. Δεν καθιστά κίνδυνο ενσωμάτωσης σε botnet	Αρνητικό
7	CVE-2017-9765	8.6	Η συγκεκριμένη ευπάθεια απευθύνεται στο πρωτόκολλο ONVIF το οποίο χρησιμοποιείται για να δώσει τη δυνατότητα σε NVR συσκευές να ενώνονται σε κάμερες από διαφορετικούς κατασκευαστές. Βασίζεται στην εκμετάλλευση του gSOAP. Μπορεί να χρησιμοποιηθεί για την εκτέλεση εντολών, αλλαγή ρυθμίσεων και λειτουργίας της κάμερας ενδεχομένως να μπορεί να κωδικοποιηθεί σε botnet.	Θετικό

Πινακας 5.6: Ευπάθειες που βρέθηκαν στη κάμερα TP-Link.

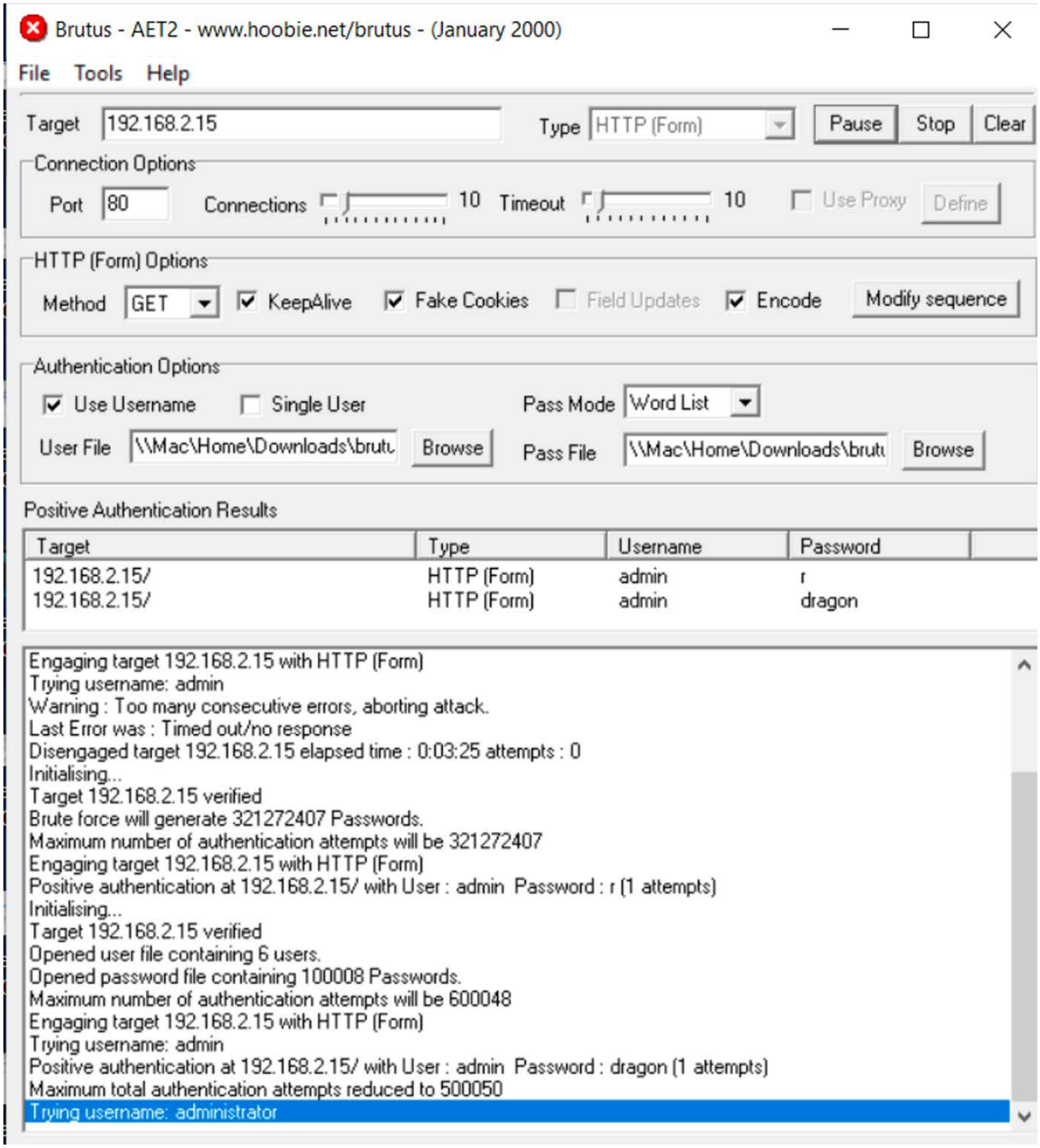
Όπως διαπιστώνεται τελικά αν και η Reolink προμηνύειτω ως η πιο ευπαθής, και το σύστημα της έχει αρκετά παλαιές ευπάθειες εν τούτοις με σωστή προετοιμασία ενδέχεται να είναι αρκετά ασφαλής σε σχέση με τις άλλες.

5.3.4 ΣΧΟΛΙΑ – ΓΕΝΙΚΟ ΣΥΜΠΕΡΑΣΜΑ.

Κάποιες από τις υποθέσεις που είχαν γίνει στο αρχικό στάδιο της έρευνας επιβεβαιώθηκαν με την εκτέλεση των δοκιμών με nmap. Υπάρχει ανοικτό το rtsp, σε κάποιες περιπτώσεις που μπορεί στην περίπτωση ανάθεσης δημόσιας διεύθυνσης IP να τύχει κατασκοπείας από επιτήδειους.
Αναθεωρώντας τα αποτελέσματα από την εκτέλεση των εντολών nmap μπορεί να γίνει η παρατήρηση πως υπάρχουν ευπάθειες οι οποίες επηρεάζουν συγκεκριμένα μοντέλα και κατασκευαστές. Συγκεκριμένα όμως και στις 3 περιπτώσεις υπάρχουν ευπάθειες οι οποίες μπορούν να παρέχουν στον επιτιθέμενο πρόσβαση στα λειτουργικά συστήματα των καμερών. Παρατηρείται πως το σχετικά καινούργιο πρωτόκολλο onVif το οποίο βασίζεται σε gSOAP αναλόγως της έκδοσης του μπορεί να τύχει τέτοιας εκμετάλλευσης. Οι εταιρίες πρέπει να είναι ιδιαίτερα προσεκτικές στην εφαρμογή του καθώς απευθύνεται σε μεγάλο πλήθος καμερών. Στο παρών στάδιο η ευπάθεια αυτή έτυχε εκμετάλλευσης από ερευνητές . Αν και δεν έχει αναφερθεί χρήση της σε exploit, θεωρητικά αυτό δεν θα αργήσει να γίνει. Συνεπώς πρέπει να μπουν μηχανισμοί οι οποίοι να επιτρέπουν την αναβάθμιση του χωρίς να επηρεάζεται το λειτουργικό σύστημα της κάμερας. Σε γενικό επίπεδο δε οι εφαρμογές πρέπει να είναι σε θέση να αναβαθμίζονται αυτόνομα στην περίπτωση που δεν επηρεάζουν την εύρυθμη λειτουργία της κάμερας.

5.4 BRUTUS AET2 PASSWORD CRACKER.

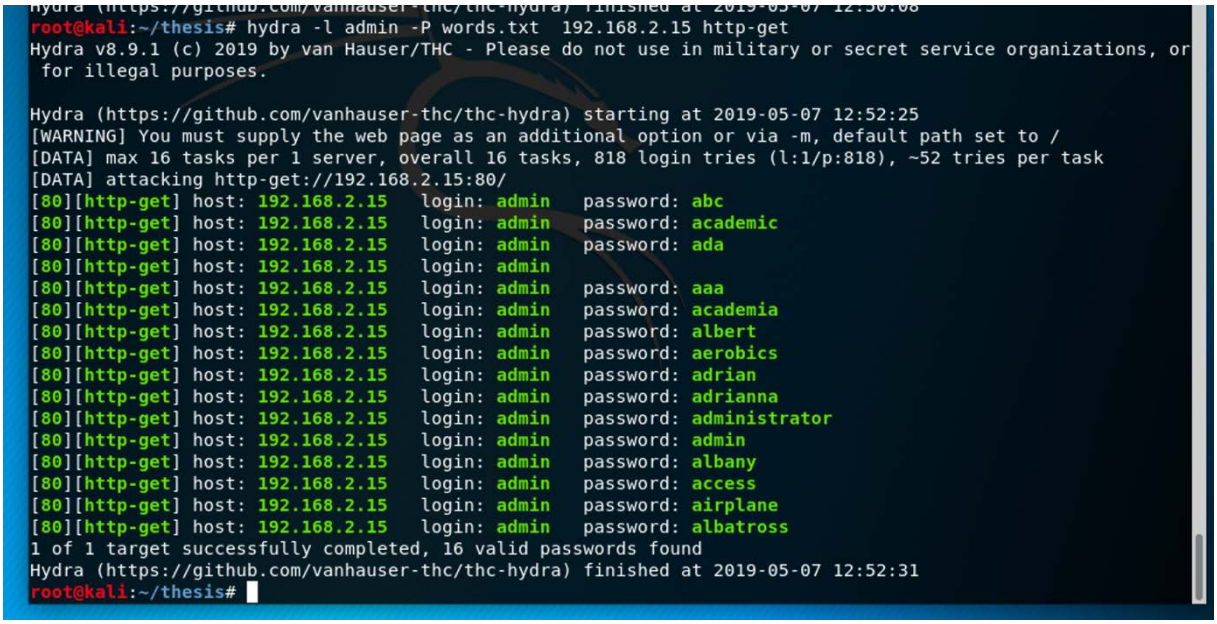
Κατά την διάρκεια της αρχικοποίησης των καμερών οι δύο εκ των τριών ζήτησαν την αλλαγή κωδικού, πράγμα θετικό, χωρίς όμως να εφαρμόσουν πολιτική εφαρμογής ισχυρού κωδικού. Υπήρχε ένδειξη που καθόριζε την πολυπλοκότητα του κωδικού, εν τούτοις ο χρήστης θα μπορούσε να επιλέξει την χρήση ενός απλού κωδικού. Με το συγκεκριμένο λογισμικό θα εξεταστεί το ενδεχόμενο κατά πόσο μπορεί να σπάσει ο κωδικός των καμερών (Th3sis!) όπου αυτός έχει εφαρμοστεί. Ενδέχεται φυσικά να είναι πιο έυκολο για την Reolink κάμερα καθώς στο παρών σημείο δεν έχει ανατεθιμένο κωδικό. Ως εκ τούτου η έρευνα θα ξεκινήσει απ' εκείνη για να καθορίσει έτσι και την αξιοπιστία του λογισμικού, καθώς αυτό έχει χαρακτηριστεί από τα καλύτερα εργαλεία σπασίματος κωδικού για το 2018.



Εικόνες 5.13: Δοκιμή σπασίματος του κωδικού με το λογισμικό Brutus-AET2.

Μετά από δοκιμές με το συγκεκριμένο λογισμικό, με διαφορετικούς συνδυασμούς ρυθμίσεων υπήρξαν αρκετά false – positives αποτελέσματα πράγμα που καθιστά το εν λόγο λογισμικό αναξιόπιστο για θέματα ανεύρεσης κωδικών. Αυτό ισχύει τουλάχιστον στο πρωτόκολλο http που χρησιμοποιούν οι κάμερες.

Για την σωστή διεκπεραίωση της δοκιμής ωστόσο έχει δοκιμαστεί και το εργαλείο hydra σε Linux. Και στην περίπτωση του hydra από 1 αρχείο με πέραν των 810 πιθανών κωδικών βρέθηκαν 16 πιθανοί κωδικοί εκ των οποίων ο 1 ήταν σωστός.



Εικόνα 5.14: Δοκιμή σπασίματος του κωδικού με το λογισμικό hydra.

5.5 MIRAI BOTNET

Όπως έχουν καταδείξει οι δοκιμές με το nmap το Mirai Botnet δεν είναι πλέον εφαρμόσιμο για τις πειραματικές δοκιμές της έρευνας. Η θύρα 23 έχει ήδη κλείσει και η υπηρεσία telnet δεν είναι πλέον διαθέσιμη σε καμία από τις 3 κάμερες. Συνεπώς η συγκεκριμένη δοκιμή δεν θα είχε κανένα νόημα σε αυτή την περίπτωση. Η αναθεώρηση των ευπαθειών τις οποίες έχει αναδείξει η δοκιμή με το nmap δεν έδειξε κάποιο άλλο διαθέσιμο botnet αυτή την στιγμή. Η κοινή ευπάθεια μέσω του πρωτοκόλλου onVif θεωρείται πολύπλοκη στην εκμετάλλευση της και δεν έχει δημιουργηθεί ακόμη στο Metasploit. Μετά από έρευνα η ευπάθεια ανακαλύφθηκε από την εταιρία Senrio η οποία αποκάλυψε την μεθοδολογία της επίθεσης χωρίς όμως να γίνεται ακριβής αναφορά. Καθώς ο σκοπός της έρευνας δεν είναι η εκμετάλλευση συγκεκριμένης ευπάθειας αλλά η αξιολόγηση της χρήσης της, μπορεί να θεωρηθεί πως υπάρχει μεγάλος βαθμός επικινδυνότητας υλοποίησης αυτής της εκμετάλλευσης σε botnet αποτεινόμενο σε συγκεκριμένους στόχους.

ΚΕΦΑΛΑΙΟ 6
Προτεινόμενο Framework

Με την ολοκλήρωση των πειραματικών δοκιμών, η έρευνα έχει παρατηρήσει πως η πλειονότητα των κατασκευαστριών εταιριών έχει αρχίσει να λαμβάνει αρκετά μέτρα ασφαλείας. Η εφαρμογή τουλάχιστον των αυτονόητων όπως την φραγή της υπηρεσίας telnet και κλείσιμο της θύρας 23. ό Επίσης η εφαρμογή πολυπλοκότητας στους αποδεκτούς κωδικούς, ή ενημέρωση στον χρήστη πως ο επιλεγμένος του κωδικός είναι αρκετά αδύναμος με εμφανή τον κίνδυνο σπασίματος του έχουν βοηθήσει αρκετά. Η χρήση δε των διακομιστών των κατασκευαστριών εταιριών για την αποστολή του video stream το οποίο μετά προωθείται στις συσκευές των χρηστών μέσω εφαρμογών αν και αποτρέπει εκμετάλλευση αδυναμιών μέσω του upnp, στους κατ' οίκον δρομολογητές εν τούτοις ελλοχεύει κινδύνους παραβίασης της ιδιωτικότητας των χρηστών από δολιοφθορά στους διακομιστές της εταιρίας τόσο από εσωτερικούς όσο και από εξωτερικούς επιτιθέμενους.

Στη συνέχεια η έρευνα θα κάνει τις δικές της προτάσεις με βάση τα ευρήματα τα οποία έχουν προκύψει από τις πειραματικές δόκιμές στην προσπάθεια ελαχιστοποίησης περαιτέρω των κινδύνων.

6.1 Λειτουργικο Συστημα.

Όπως έχει παρατηρηθεί μέσω των πειραματικών δοκιμών οι δικτυακές κάμερες χρησιμοποιούν λειτουργικά βασισμένα σε εκδόσεις Linux με περιορισμένα πακέτα για σκοπούς εξοικονόμησης πόρων (επεξεργαστή και μνήμης). Είναι δε εμφανές ότι σε αρκετές περιπτώσεις οι κάμερες δεν τυγχάνουν συχνής ενημέρωσης των λειτουργικών τους πράγμα που τις αφήνει τρωτές σε τυχόν ευπάθειες οι οποίες ανακαλύπτονται κατά καιρούς. Καθώς οι αναβαθμίσεις του λειτουργικού συστήματος προϋποθέτουν την εγγραφή στην EEPROM μνήμη δεν είναι κάτι το οποίο μπορεί να θεωρηθεί εύκολο ή να αυτοματοποιηθεί λόγο των κινδύνων να χαλάσει η κάμερα. Το θετικό κομμάτι είναι πως λόγο του ότι το λειτουργικό είναι εγκατεστημένο σε Read Only μνήμη, τυχόν αλλαγές τις οποίες μπορεί να κάνει ένα botnet υφίστανται μέχρι την επανεκκίνηση της κάμερας. Κατά συνέπεια η έρευνα επικροτεί την εφαρμογή αυτόματης επανεκκίνηση των καμερών σε εβδομαδιαία βάση, ενδεχομένως σε μέρα και ώρα που θα επιλέξει ο χρήστης. Συνήθως μια

επανεκκίνηση δεν παίρνει πέραν των 2 λεπτών, απώλεια χρήσης που είναι αποδεκτή από τον οποιοδήποτε οικιακό χρήστη. Καθώς η χρήση μιας προσβεβλημένης κάμερας σε επίθεση, από την μέρα προσβολής της, μπορεί να πάρει αρκετό καιρό η μέθοδος αυτή μειώνει τις πιθανότητες η κάμερα να είναι υπό την επήρεια του botnet όταν ο control server δώσει την εντολή για επίθεση. Η τεχνική αυτή ήδη υφίσταται στο firmware της κάμερας TP-Link, αλλά δεν είναι ενεργοποιημένη από προεπιλογή. Συστήνεται η ενεργοποίηση και εφαρμογή της σαν προεπιλογή έτσι ώστε παρασχεθεί ένα επιπρόσθετο μέτρο αντίδρασης στην περίπτωση που προσβληθεί. .

6.2 WEB SERVER.

Η συνήθης επικοινωνία στο διαδίκτυο για μετάδοση πληροφοριών και δεδομένων είναι μέσω ιστοσελίδων. Η έκδοση του web server που είναι εγκατεστημένος στο οποιοδήποτε πληροφοριακό σύστημα ενδέχεται να αποκαλύψει τις διάφορες ευπάθειες στις οποίες υπόκειται το συγκεκριμένο σύστημα. Καθώς είναι το λογισμικό το οποίο εξυπηρετεί την επικοινωνία μεταξύ του διακομιστή και του πελάτη αρκετά συχνά αποτελεί το τρωτό σημείο εισόδου σε ένα σύστημα. Αυτό μπορεί να συμβαίνει είτε λόγο κάποιου bug το οποίο έχει στην υλοποίηση του λογισμικού, ή κάποιο από τα προστιθέμενα προγράμματα του (πχ php, sql-plugin) ή ακόμα και προβλήματος της ιστοσελίδας την οποία φιλοξενεί η οποία να αφήνει ανοικτά τρωτά σημεία για είσοδο στο σύστημα. Η έκδοση του του web server μπορεί να δώσει στον επιτιθέμενο αρκετές πληροφορίες σχετικά με τις ευπάθειες στις οποίες ενδεχομένως να υπόκειται τόσο αυτός όσο και τα plugins του. Συνήθως οι web server είναι συμβατοί με τις προηγούμενες εκδόσεις τους, οπόταν οι κατασκευάστριες εταιρίες συνιστάται να προβαίνουν σε ενημερώσεις των web-servers τουλάχιστον μια φορά τον χρόνο έστω και αν είναι οι μόνες εφαρμογές οι οποίες αναβαθμίζονται σε ένα λειτουργικό και κυκλοφορία του αναβαθμισμένου λειτουργικού.

6.3 ΚΡΥΠΤΟΓΡΑΦΙΑ.

Έχει γίνει η παρατήρηση πως αν και οι κάμερες υποστηρίζουν κρυπτογραφικά το SSL για ασφαλή ενώσεις μέσω https εν τούτοις τα πιστοποιητικά τα οποία ανταλλάζονται είναι self-signed. Αυτό κάνει τις δικτυακές κάμερες τρωτές σε επιθέσεις Man in the Middle, όπου ο χρήστης μπορεί εν αγνοία του να παραχωρήσει τους κωδικούς του στον επίδοξο εισβολέα με ότι συνέπειες μπορεί αυτό να αποφέρει.

Ως εκ τούτου η έρευνα προτείνει την αγορά wildcard διεθνώς αναγνωρισμένων πιστοποιητικών από τις κατασκευάστριες εταιρίες. Έτσι θα τους δωθεί η δυνατότητα έκδοσης αναγνωρισμένου πιστοποιητικού, το οποίο ο φυλλομετρητής του χρήστη θα εμπιστεύεται εκ των προτέρων χωρίς την ανάγκη εκχώρησης exception. Καθώς η διαδικασία πιστοποίησης και έκδοσης

πιστοποιητικού είναι συνυφασμένη με την διεύθυνση IP ενός συστήματος συστήνεται το εξής flowchart βάση του οποίου μπορούν να εκδίδονται τα πιστοποιητικά με βάση την διευθυνσιοδότηση IPv4.

Η εταιρία διατηρεί μια βάση δεδομένων στην οποία είναι καταγεγραμμένα τα στοιχεία της κάθε κάμερας την οποία κατασκευάζει όπου συμπεριλαμβάνονται το μοντέλο, serial number και το MAC address της κάθε κάμερας.

Η κάμερα εκκινά και λαμβάνει διεύθυνση μέσω DHCP από τον router του ιδιοκτήτη. Μέρος της διαδικασίας εκκίνησης είναι η δημιουργία ενός CSR (Certificate Signing Request) το οποίο αποστέλλεται στον CA (Certificate Authority) της κατασκευάστριας εταιρίας. Ο CA δημιουργεί το certificate και το αποστέλλει πίσω στην κάμερα προς εγκατάσταση ενώ έχει ήδη στα στοιχεία του το εσωτερικό (private) και εξωτερικό (public) IP address της κάμερας. Καταχωρεί το εν λόγο πιστοποιητικό στη βάση δεδομένων με τα στοιχεία της κάμερας. Κάθε φορά που έρχεται καινούργιο CSR από την κάμερα λόγο αλλαγής της διεύθυνσης IP ο CA δημιουργεί καινούργιο Certificate και σβήνει το παλιό. Στην περίπτωση που τα στοιχεία είναι τα ίδια μπορεί ή να αγνοήσει το CSR ή να στείλει πίσω το παλαιό πιστοποιητικό. Η εν λόγο διαδικασία ή τουλάχιστον παραλλαγή της θα δημιουργήσει ένα αρκετά δυνατό κρυπτογραφικό δεσμό μεταξύ της κάμερας, της εταιρίας κατασκευής και του ιδιοκτήτη ο οποίος μπορεί πλέον να χρησιμοποιήσει τη συσκευή του έχοντας την βεβαιότητα ότι κανείς δεν υποκλέπτει την επικοινωνία τους.

Αυτό φυσικά επιφέρει επιπλέον οικονομικά κόστη στους κατασκευαστές οι οποίοι θα πρέπει να γίνουν trusted CA Authorities ή να αγοράσουν wildcard certificates μεγέθους ανάλογο με τις πωλήσεις τους, τα οποία πιθανό να μετακυλήσουν στο κόστος κατασκευής και διάθεσης της δικτυακής κάμερας.

6.4 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ.

Το συγκεκριμένο μέτρο ασφαλείας δεν έχει να κάνει με την κάμερα και την λειτουργικότητα της καθ' εαυτό, αλλά με το περιβάλλον στο οποίο θα εγκατασταθεί η κάμερα. Εάν ο χρήστης δεν είναι γνώστης του πως μπορεί να ασφαλίσει επιτυχώς τη συσκευή του πρέπει να υπάρχει η ανάλογη προστασία από το περιβάλλον στο οποίο θα εγκατασταθεί. Κατά συνέπεια η κάμερά δικτυακά, πρέπει να εγκαθίσταται πίσω από τοίχος προστασίας το οποίο να φιλτράρει την πρόσβαση στις υπηρεσίες της κάμερας από το διαδίκτυο. Το ιδανικό σενάριο προϋποθέτει όπως η κάμερα έχει ιδιωτική διεύθυνση IP και πρόσβαση στο διαδίκτυο μέσω NAT εάν αυτή είναι απολύτως απαραίτητη. Συνιστάται η κάμερα να μην έχει πρόσβαση από ή προς το διαδίκτυο, αντιθέτως με την υποστήριξη του πρωτοκόλλου onVif οι κάμερες θα μπορούσαν να ενωθούν με το ευπαθές πρωτόκολλο σε ένα NVR ,των οποίων η ευπάθειες δεν απασχόλησαν την παρούσα έρευνα.Γίνεται

όμως η υπόθεση πως από τη στιγμή που τα NVR έχουν πιο πολλούς υπολογιστικούς πόρους μπορούν να αποτελέσουν ασφαλέστερα συστήματα με λιγότερες ευπάθειες. Πρόσβαση στο NVR δίνει πρόσβαση στην εικόνα της και βασική της χρήση, χωρίς ωστόσο να την εκθέτει καθ' εαυτό σε κίνδυνο.

6.5 ΠΑΡΑΒΙΑΣΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ.

Η συγκεκριμένη κατηγορία αδυναμιών δεν συνιστά κίνδυνο εκμετάλλευσης από κάποιο botnet. Γίνεται όμως αναφορά καθώς η χρήση των πρωτοκόλλων rtmp και rtsp χωρίς την χρήση authentication συνιστά κινδύνους στην παραβίαση της ιδιωτικότητας των χρηστών. Η παραβίαση της ιδιωτικότητας των χρηστών μπορεί να έχει μεγάλο οικονομικό και αισθηματικό κόστος. Καθώς το rtsp χρησιμποποιεί UDP για την αποστολή των πακέτων προς τον παραλήπτη είναι εμφανές πως τυχόν πακέτα τα οποία αναχαιτιστούν, μπορούν να επανασταλούν από τον επίδοξο hacker με απώτερο σκοπό την παραποίηση / προσβολή της αξιοπιστίας των δεδομένων τα οποία στέλνει η κάμερα. Ως εκ τούτου συστήνεται η χρήση του RTMPs για την αποστολή video το οποίο μεταξύ άλλων χρησιμοποιεί TCP για την αποστολή των πακέτων. Στο TCP υπάρχει η δυνατότητα χρήσης timestamp για όπου το κάθε πακέτο έχει την χρονική στιγμή την οποία στάλθηκε όπως επίσης και την χρονική περίοδο για την οποία το πακέτο θεωρείται έγκυρο συνεπώς είναι πιο ανθεκτικό στις προαναφερθείσες επιθέσεις. Συνεπώς η χρήση του RTMPS το οποίο υποστηρίζει την χρήση TLS/SSL για την κρυπτογράφηση της εικόνας της οποίας στέλνει η κάμερα, μαζί με τα timestamps και την χρήση authentication ελαχιστοποιούν τις πιθανότητες παραβίασης τόσο της ιδιωτικότητας του χρήστη αλλά αυξάνει και την αξιοπιστία της εικόνας που στέλνει η κάμερα.

6.6 ΕΚΤΙΜΗΣΗ ΕΠΙΚΥΝΔΙΝΟΤΗΤΑΣ.

Για σκοπούς ενημέρωσης του χρήστη ή έρευνα έχει αναπτύξει ένα λογισμικό το οποίο έχει σκοπό να ενημερώσει τον χρήστη για το ποσοστό ασφάλειας το οποίο διακατέχει την συσκευή του σε σχέση με τις ρυθμίσεις τις οποίες έχει εφαρμόσει. Το πρόγραμμα βασίζεται σε μια σειρά ερωτήσεων οι οποίες έχουν ξεχωριστή βαρύτητα σε σχέση με την ασφάλεια της κάμερας:

1. Password Strength: Πολυπλοκότητα κωδικού. Η παράμετρος αυτή καθορίζεται όπως παρατηρήθηκε από τις κάμερες Foscam και TP-Link από το μέγεθος του κωδικού, την χρήση συνδυασμού κεφαλαίων – πεζών γραμμάτων, με αριθμούς και σημεία στίξης. Η παράμετρος αυτή συνιστά το 25% της ολικής βαθμολογίας. Με δυνατό κωδικό

    1.1. Δυνατός Κωδικός: 25 μονάδες

    1.2. Μεσαίας Δύναμης Κωδικός: 15 μονάδες

    1.3. Αδύνατος Κωδικός: 5 μονάδες

2. Έμπιστο πιστοποιητικό: Καθώς οι πλείστες δικτυακές κάμερες προσφέρουν self-signed πιστοποιητικά SSL, είναι αρκετά εύκολο ο χρήστης τους να πέσει θύμα επίθεσης Man In the Middle. Συνεπώς στην περίπτωση που υπάρχει υποστήριξη χρήσης έμπιστου πιστοποιητικού από Αναγνωρισμένο Certificate Authority προσφέρει προστασία από τέτοιου είδους επιθέσεις. Ο τομέας αυτός συνιστά το 15% της βαθμολογίας της κάμερας καθώς ο επιτιθέμενος θα πρέπει να αποκτήσει πρόσβαση και στο δίκτυο του χρήστη για να μπορέσει να επιτελέσει την επίθεση.

3. Πρόσβαση από και Προς το Διαδίκτυο. Λαμβάνεται υπόψη κατά πόσο η δικτυακή κάμερα είναι προσβάσιμη μόνο στο τοπικό δίκτυο ή αν υπάρχει και πρόσβαση από το διαδίκτυο. Θεωρείται ο παραγόντας με την περισσότερη βαρύτητα (40%) καθώς κάτι το οποίο δεν είναι προσβάσιμο δεν μπορεί να πέσει και θύμα επίθεσης ή εκμετάλλευσης. Εάν ο χρήστης δεν είναι γνώστης του πως να ασφαλίσει την κάμερα του μέσω NAT (Network Address Translation) ή firewall, καλύτερα να μην είναι προσβάσιμη από το διαδίκτυο.

4. Εβδομαδιαία Αυτόματη Επανεκκίνηση: Όπως αναφέρθηκε τα botnets μετά που προσβάλλουν τους στόχους τους, εργάζονται από τη RAM του θύματος τους χωρίς να έχουν την δυνατότητα εγγραφής στο EEPROM της συσκευής. Κατά συνέπεια ακόμα και να προσβληθεί μια κάμερα από κάποιο botnet η επανεκκίνηση της θα το διαγράψει επαναφέροντας την σε καθαρή κατάσταση. Η συγκεκριμένη ρύθμιση προσθέτει 20% στην ασφάλεια της κάμερας.

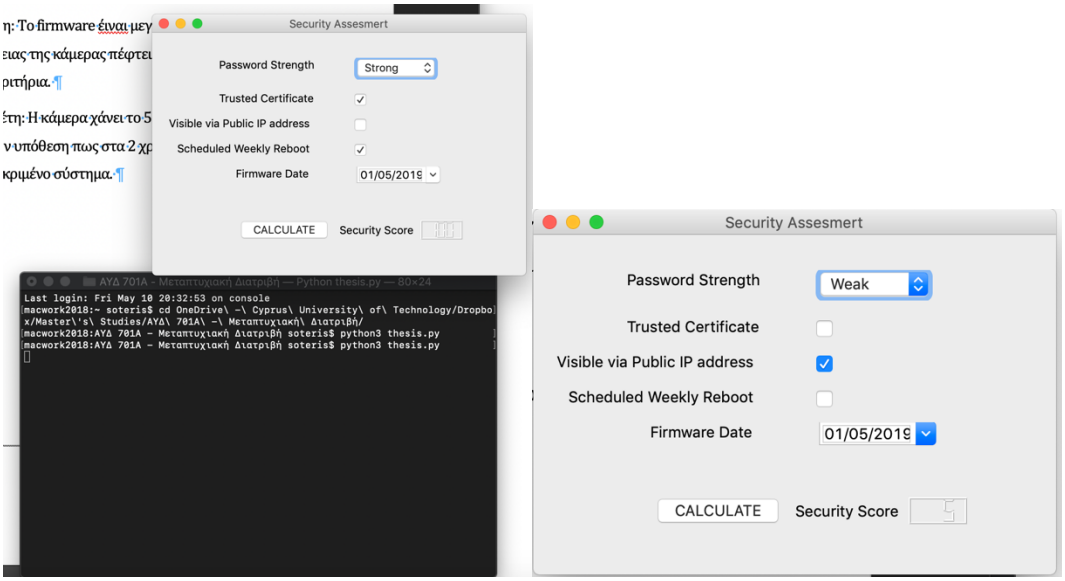
5. Ημερομηνία έκδοσης λειτουργικού συστήματος της κάμερας: Αρκετές φορές τα μέτρα ασφαλείας του παρόντος καταλήγουν παρωχημένα σε διάστημα 2-3 χρόνων είναι εμφανές

πως εάν ένα πληροφοριακό σύστημα δεν αναβαθμιστεί με το πέρας του χρόνου θα καταστεί ευάλωτο. Αυτό προκύπτει από την ανακάλυψη νέων ευπαθειών, αύξηση της υπολογιστικής δύναμης των επιτιθέμενων για brute force attacks κ.ο.κ.. Η παράμετρος αυτή θεωρείται πως δρα ποσοστιαία στην εκτίμηση της ασφάλειας με την εξής εξήγηση:

5.1. Το firmware είναι μικρότερο από 1 έτος: Η κάμερα διατηρεί την βαθμολογία που πήρε από τα 4 κριτήρια που αναφέρθηκαν πιο πάνω.

5.2. Το firmware είναι μικρότερο από 2 έτη: Το firmware είναι μεγαλύτερο από 1 έτος αλλά μικρότερο από 2. Το ποσοστό ασφάλειας της κάμερας πέφτει κατά 10% από την βαθμολογία την οποία πήρε από τα κριτήρια.

5.3. Το firmware είναι μεγαλύτερο από 2 έτη: Η κάμερα χάνει το 50% της βαθμολογίας που πήρε από τα κριτήρια, βασισμένο στην υπόθεση πως στα 2 χρόνια ενδέχεται να βρεθεί ευπάθεια που θα επηρεάσει το συγκεκριμένο σύστημα.



Εικόνες 6.1: Εικόνες απλο το λογισμικό που αναπτύχθηκε.

Το λογισμικό αναπτύχθηκε χρησιμοποιώντας την γλώσσα προγραμματισμού python ενώ για το γραφικό περιβάλλον χρησιμοποιήθηκε το QT Designer για python. Παρατίθενται πιο κάτω ο πηγαίος κώδικας τόσο για το γραφικό περιβάλλον όσο και για τη λειτουργικότητα του προγράμματος:

Μετά την δημιουργία του γραφικού περιβάλλοντος, για να μεταφραστεί σε κώδικα python δίνουμε την εντολή:

pyuic5 Security_Assesment.ui -o Security_Assesment.py

Security_Assesment.py:

```
macwork2018:ΑΥΔ 701Α - Μεταπτυχιακή Διατριβή soteris$ cat Security_Assesment.py
# -*- coding: utf-8 -*-

# Form implementation generated from reading ui file 'Security_Assesment.ui'
#
# Created by: PyQt5 UI code generator 5.12.2
#
# WARNING! All changes made in this file will be lost!

from PyQt5 import QtCore, QtGui, QtWidgets


class Ui_Security(object):
  def setupUi(self, Security):
    Security.setObjectName("Security")
    Security.resize(447, 290)
    self.lbl_pass = QtWidgets.QLabel(Security)
    self.lbl_pass.setGeometry(QtCore.QRect(80, 30, 131, 16))
    self.lbl_pass.setObjectName("lbl_pass")
    self.passPower = QtWidgets.QComboBox(Security)
    self.passPower.setGeometry(QtCore.QRect(240, 30, 104, 26))
    self.passPower.setMaxVisibleItems(3)
    self.passPower.setObjectName("passPower")
    self.passPower.addItem("")
    self.passPower.addItem("")
    self.passPower.addItem("")
    self.ssl_trust = QtWidgets.QCheckBox(Security)
    self.ssl_trust.setGeometry(QtCore.QRect(240, 70, 87, 20))
    self.ssl_trust.setText("")
    self.ssl_trust.setChecked(True)
    self.ssl_trust.setObjectName("ssl_trust")
    self.lbl_cert = QtWidgets.QLabel(Security)
    self.lbl_cert.setGeometry(QtCore.QRect(80, 70, 121, 16))
    self.lbl_cert.setObjectName("lbl_cert")
    self.lbl_reboot = QtWidgets.QLabel(Security)
    self.lbl_reboot.setGeometry(QtCore.QRect(30, 130, 181, 16))
    self.lbl_reboot.setObjectName("lbl_reboot")
    self.lbl_date = QtWidgets.QLabel(Security)
    self.lbl_date.setGeometry(QtCore.QRect(100, 160, 141, 16))
    self.lbl_date.setObjectName("lbl_date")
    self.firmware_date = QtWidgets.QDateEdit(Security)
    self.firmware_date.setGeometry(QtCore.QRect(240, 160, 110, 21))
    self.firmware_date.setMaximumDate(QtCore.QDate(2020, 12, 31))
    self.firmware_date.setMinimumDate(QtCore.QDate(2015, 1, 1))
    self.firmware_date.setCalendarPopup(True)
    self.firmware_date.setDate(QtCore.QDate(2019, 5, 1))
    self.firmware_date.setObjectName("firmware_date")
    self.public_ip = QtWidgets.QCheckBox(Security)
    self.public_ip.setGeometry(QtCore.QRect(240, 100, 87, 20))
    self.public_ip.setText("")
    self.public_ip.setObjectName("public_ip")
    self.reboot_wkl = QtWidgets.QCheckBox(Security)
    self.reboot_wkl.setGeometry(QtCore.QRect(240, 130, 87, 20))
    self.reboot_wkl.setText("")
```

```
        self.reboot_wkl.setChecked(True)
        self.reboot_wkl.setObjectName("reboot_wkl")
        self.lbl_IP = QtWidgets.QLabel(Security)
        self.lbl_IP.setGeometry(QtCore.QRect(20, 100, 201, 16))
        self.lbl_IP.setObjectName("lbl_IP")
        self.layoutWidget = QtWidgets.QWidget(Security)
        self.layoutWidget.setGeometry(QtCore.QRect(100, 220, 271, 35))
        self.layoutWidget.setObjectName("layoutWidget")
        self.horizontalLayout = QtWidgets.QHBoxLayout(self.layoutWidget)
        self.horizontalLayout.setContentsMargins(0, 0, 0, 0)
        self.horizontalLayout.setObjectName("horizontalLayout")
        self.calculate = QtWidgets.QPushButton(self.layoutWidget)
        self.calculate.setObjectName("calculate")
        self.horizontalLayout.addWidget(self.calculate)
        self.label = QtWidgets.QLabel(self.layoutWidget)
        self.label.setObjectName("label")
        self.horizontalLayout.addWidget(self.label)
        self.sec_score = QtWidgets.QLCDNumber(self.layoutWidget)
        font = QtGui.QFont()
        font.setBold(True)
        font.setWeight(75)
        font.setStrikeOut(False)
        self.sec_score.setFont(font)
        self.sec_score.setDigitCount(3)
        self.sec_score.setProperty("value", 100.0)
        self.sec_score.setObjectName("sec_score")
        self.horizontalLayout.addWidget(self.sec_score)

        self.retranslateUi(Security)
        QtCore.QMetaObject.connectSlotsByName(Security)

    def retranslateUi(self, Security):
        _translate = QtCore.QCoreApplication.translate
        Security.setWindowTitle(_translate("Security", "Security Assesmert"))
        self.lbl_pass.setText(_translate("Security", "Password Strength"))
        self.passPower.setItemText(0, _translate("Security", "Strong"))
        self.passPower.setItemText(1, _translate("Security", "Medium"))
        self.passPower.setItemText(2, _translate("Security", "Weak"))
        self.lbl_cert.setText(_translate("Security", "Trusted Certificate"))
        self.lbl_reboot.setText(_translate("Security", "Scheduled Weekly Reboot"))
        self.lbl_date.setText(_translate("Security", "Firmware Date"))
        self.lbl_IP.setText(_translate("Security", "Visible via Public IP address"))
        self.calculate.setText(_translate("Security", "CALCULATE"))
        self.label.setText(_translate("Security", "Security Score"))
```

thesis.py:

```
macwork2018:ΑΥΔ 701Α - Μεταπτυχιακή Διατριβή soteris$ cat thesis.py
#Importing Required Classes and Modules

import sys
from datetime import date
from time import strftime
from PyQt5 import QtWidgets
from PyQt5 import QtGui
from PyQt5 import QtCore, uic

# Import the GUI of the script created with QtDesigner
from Security_Assesment import Ui_Security

class thesis(QtWidgets.QMainWindow):

    def __init__(self):
        super(thesis, self).__init__()
        self.ui = Ui_Security()
        self.ui.setupUi(self)

# Procedure to calculate the security level of the camera

def secure_calc():
    today = date.today()
    firm_date = window.ui.firmware_date.date().toPyDate()
    if (str(window.ui.passPower.currentText()) == "Medium"):
        password = 15
    else:
        if (str(window.ui.passPower.currentText()) == "Weak"):
            password = 5
        else:
            password = 25
    if (window.ui.ssl_trust.isChecked() == False):
        certificate = 0
    else:
        certificate = 15
    if (window.ui.public_ip.isChecked() == True):
        internet_access = 0
    else:
        internet_access = 40
    if (window.ui.reboot_wkl.isChecked() == False):
        weekly_reboot = 0
    else:
        weekly_reboot = 20
    if ((today - firm_date).days < 365):
            multiplier = 1
    else:
        if ((today - firm_date).days < 730):
            multiplier = 0.9
```

```
        else:
            multiplier = 0.5

    score = password + certificate + internet_access + weekly_reboot
    lcd = score * multiplier
    window.ui.sec_score.intValue = lcd
    window.ui.sec_score.display(lcd)
    window.ui.sec_score.hide()
    window.ui.sec_score.show()
    window.show()

# Initialise the application

app = QtWidgets.QApplication([])
window = thesis()
window.ui.calculate.clicked.connect(secure_calc)
window.show()

#Initialise Variables

score = 0
password = 25
certificate = 15
internet_access = 40
weekly_reboot = 20
multiplier = 1
sys.exit(app.exec_())
```

ΚΕΦΑΛΑΙΟ 7
Επίλογος

Ολοκληρώνοντας η έρευνα συνοψίζει παρακάτω τα συμπεράσματα της αναφέροντας επίσης τις προκλήσεις τις οποίες αντιμετώπισε καθώς επίσης και πιθανές παραλείψεις. Στη συνέχεια γίνονται προτάσεις που αφορούν μελλοντική εργασία η οποία θα μπορεί να προστεθεί στο παρών ερευνητικό έργο

7.1 ΣΥΜΠΕΡΑΣΜΑ.

Με την ολοκλήρωση της ερευνητικής δραστηριότητας μπορούν να εξαχθούν ορισμένα συμπεράσματα τα οποία θα βοηθήσουν την ερευνητική κοινότητα, στην αντιμετώπιση των απειλών οι οποίες υφίστανται σήμερα. Μελλοντικές εργασίες θα μπορούν να αξιοποιήσουν την μεθοδολογία και τα παρών ευρήματα για επιβεβαίωση και εμβάθυνση επ' αυτών.

Είναι εμφανές πως οι μετά τα τεράστια πλήγματα τα οποία προξένησαν οι επιθέσεις με την χρήση του Mirai botnet και των παραλλαγών του, οι κατασκευάστριες εταιρίες, τουλάχιστον των δικτυακών καμερών, άρχισαν να παίρνουν μέτρα και να ασφαλίζουν τις συσκευές τους. Βάση των μέτρων αυτών :

- Δεν υποστηρίζεται πλέον η χρήση του πρωτοκόλλου telnet και έκλεισε η θύρα 23
- Απαιτείται η αλλαγή του κωδικού πρόσβασης με ένδειξη του δείκτη ασφαλείας του και σε κάποιες περιπτώσεις ακόμα και το όνομα χρήστη προς αποφυγή σύνδεσης συνδυασμού διαπιστευτηρίων με συγκεκριμένη κατασκευάστρια εταιρία.
- Σε ορισμένες περιπτώσεις δεν χρησιμοποιούνται οι ενδεδειγμένες θύρες για την παροχή ορισμένων υπηρεσιών προς απόκρυψη τους από αυτοματοποιημένες ανιχνεύσεις.

Ενώ τα μέτρα αυτά σίγουρα έχουν μειώσει την ευκολία με την οποία μπορούν οι συγκεκριμένες συσκευές να προσβληθούν από botnets εν τούτοις παρατηρείται πως δεν την έχουν εξαλείψει τελείως. Στον τομέα της ασφάλειας των πληροφοριακών συστημάτων χρειάζεται συνεχόμενη προσπάθεια εύρεσης και εφαρμογής διορθώσεων σε μορφή αναβάθμισης λειτουργικού και (firmware updates) και απαλοιφή λαθών κώδικα από τις κατασκευάστριες εταιρίες.

Υπάρχουν επίσης ευπάθειες και αδυναμίες των οποίων η λύση είναι πολυσύνθετη όπως αυτή της κρυπτογραφίας και παραβίασης της ιδιωτικότητας. Η έρευνα έχει προσφέρει κάποιες εισηγήσεις ως προς τον τρόπο αντιμετώπισης τους, εν τούτοις απέφυγε να εμβαθύνει επ' αυτών καθώς παρέκκλιναν από τον αρχικό στόχο της.

7.2 ΜΕΛΛΟΝΤΙΚΗ ΕΡΓΑΣΙΑ.

Η μελέτη αυτή μπορεί να συνεχιστεί με το ενδεχόμενο εκμετάλλευσης της αδυναμίας η οποία εντοπίστηκε στο πρωτόκολλο onVIF και πιθανή ενσωμάτωση της σε botnet εντός εργαστηριακού περιβάλλοντος έτσι ώστε να μπορούν να σχεδιαστούν ή να προταθούν τα κατάλληλα μέτρα προστασίας προτού γίνει το επόμενο Mirai. Εξ' όσον έχει γίνει γνωστό το gSOAP χρησιμοποιείται και σε συσκευές πέραν των δικτυακών καμερών κατά συνέπεια αυξάνοντας το πλήθος των πιθανών στόχων.

Επίσης το λογισμικό το οποίο αναπτύχθηκε θα μπορούσε να ενσωματωθεί σε λειτουργικό σύστημα κάμερας έτσι ώστε να παρέχεται σε πραγματικό χρόνο το επίπεδο ασφαλείας της κάμερας κατά την διάρκεια της ρύθμισης της.

Σαν μελλοντικό εγχείρημα όμως μπορεί να αποτελέσει και η συνεχής ανάπτυξη του προτεινόμενου λογισμικού με την προσθήκη λειτουργικότητας των ελέγχων nmap, API για έλεγχο μέσω της μηχανής αναζήτησης Shodan και λειτουργικότητα tcpdump για έλεγχο του επιπέδου ασφαλείας με περισσότερη ακρίβεια σε πραγματικό χρόνο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Albrecht, Katherine, and Liz McIntyre. 2015. "Privacy Nightmare: When Baby Monitors Go Bad [Opinion]." *IEEE Technology and Society Magazine* 34(3): 14–19.

Angrishi, Kishore. 2017. *Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets*. www.amazon.com (October 14, 2018).

Antonakakis, Manos et al. *Understanding the Mirai Botnet*. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis (October 14, 2018).

Behniafar, Morteza, Alireza Nowroozi, and Hamid Reza Shahriari. 2018. 10 *A Survey of Anomaly Detection Approaches in Internet of Things*. http://www.isecure-journal.org (December 5, 2018).

Botnet, An Adaptive Peer-to-peer, and Vladimir Diaconescu. "Hide ' n ' Seek."

Boyarinov, Konstantin, and Aaron Hunter. 2017. "Security and Trust for Surveillance Cameras." *2017 IEEE Conference on Communications and Network Security, CNS 2017* 2017-Janua: 384–85.

Bugeja, Joseph, Désirée Jönsson, and Andreas Jacobsson. 2018. "An Investigation of Vulnerabilities in Smart Connected Cameras." *2018 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2018*: 537–42.

"Denial of Service Attack | Definition & Facts | Britannica.Com." https://www.britannica.com/technology/denial-of-service-attack (December 4, 2018).

Edwards, Sam, and Ioannis Profetis. 2016. "Hajime: Analysis of a Decentralized Internet Worm for IoT Devices." https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf.

Karasaridis, Anestis, Brian Rexroad, and David Hoeflin. *Wide-Scale Botnet Detection and Characterization*. http://static.usenix.org/events/hotbots07/tech/full_papers/karasaridis/karasaridis.pdf (November 6, 2018).

Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. "DDoS in the IoT: Mirai and Other Botnets." *Computer* 50(7): 80–84.

Kramer, Simon, and Julian C Bradfield. 2010. "A General Definition of Malware." *J Comput Virol* 6: 105–14. https://link.springer.com/content/pdf/10.1007%2Fs11416-009-0137-1.pdf (November 4, 2018).

Schach, Stephen R. 2017. "OO Analysis OBJECT-ORIENTED ANALYSIS OO Analysis." : 1–27.

Schuba, Christoph L et al. 1997. "Coronary Sinus and Fossa Ovalis Ablation.Pdf."

Seralathan, Yogeesh et al. 2018. "IoT Security Vulnerability□: A Case Study of a Web Camera." : 172–77.

Tekeoɔlu, Ali, and Ali Şaman Tosun. 2015. "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam." *Proceedings - International Conference on Computer Communications and Networks, ICCCN* 2015-Octob.

Weyrich, Michael, and Christof Ebert. 2016. "Reference Architectures for the Internet of Things." *IEEE Software* 33(1): 112–16.

ΠΑΡΑΡΤΗΜΑ Α
Τίτλος Παραρτήματος

Τα παραρτήματα αριθμούνται με ελληνικά κεφαλαία γράμματα.

Α.1 ΠΡΟΔΙΑΓΡΑΦΕΣ ΚΑΜΕΡΩΝ

Α.1.1 FOSCAM R2

ITEMS		R2
Image Sensor	Sensor Type	1/2.7" CMOS
	Display Resolution	2.0MegaPixels (1920*1080)
	Frame Rate	25fps
	Min. Illumination	0 Lux (With IR Illuminator)
Lens	Lens Type	f:2.8mm,F:2.6
	Angle of View	Horizontal:95° Diagonal : 100°
	Night Vision	13pcs IR-LEDs, night vision range up to 8 meters
Video	Image Compression	H.264
	Resolution	1080P(1920x1080) ,720P(1280 x 720), VGA(640 x 480), QVGA(320 x 240)
	Stream	dual stream
	Image adjustment	The hue, brightness, contrast, saturation, sharpness are adjustable
	Flip image	flip and mirror
	Infrared mode	Automatic or manual
	Pan/Tilt Angle	Horizontal:350° & Vertical: 100°
	Night visibility	13pcs IR-LEDs, night vision range up to 8 metres
Audio	Input/Output	Supports two-way audio Built-in Mic & Speaker
Network	Ethernet	One 10/100Mbps RJ45 port
	Wireless Standard	IEEE802.11b/g/n
	Data Rate	IEEE802.11b: 11Mbps(Max.); IEEE802.11g: 54Mbps(Max.); IEEE802.11n: 150Mbps(Max.).
	Wireless Security	WEP, WPA, WPA2
	Wireless Setup	Supports EZLink wireless setup
	Network Protocol	IP、TCP、UDP、HTTP、HTTPS、SMTP、FTP、DHCP、DDNS、UPnP、RTSP、WPS、ONVIF
	Remote Access	P2P, DDNS
System Requirements	Operating System	Microsoft Windows XP, 7, 8;Mac OS;iOS、Android
	Browser	Microsoft IE8 and above version or compatible browser; Google Chrome; Apple Safari.
Other Features	Motion Detection	Alarm via E-Mail, upload alarm snapshot to FTP
	Sound Detection	Alarm via E-Mail, upload alarm snapshot to FTP
	HDR	Improve image clarity in complex scenario
	Magic Zoom	A Magic digital zoom function rivaled Optical zoom
	User Accounts	Three levels user role
	Firewall	Supports IP Filtering
	Storage	128G Micro SD card, local and FTP storage
	Reset	Reset button is available
Power	Power Supply	DC 5V/2.0A
	Power Consumption	<6W
Physical	Dimension(mm)	74(L)×74(W)×119(H)
	Net Weight	290g
Environment	Operating Temperature	-10°C ~ 50° (14°F ~ 122°F)
	Operating Humidity	20% ~ 85% non-condensing
	Storage Temperature	-20°C ~ 60° (-4°F ~ 140°F)
	Storage Humidity	0% ~ 90% non-condensing
Certification	CE, FCC, RoHS	

A.1.2 TP-LINK 450

Specifications

Camera

- **Image Sensor:** 1/4" progressive scan CMOS sensor
- **Resolution:** 1.0 Megapixel (1280 x 720)
- **Lens:** F: 2.0, f: 3.6 mm
- **Viewing Angle:** FOV = 75°, see up to 360/150 degrees with Pan/Tilt
- **Night Vison:** 850 nm LEDs brighten up to 26 feet

Audio

- **Audio Communication:**
  2-way audio
  Adjustable audio alerts
- **Audio Input:** Built-in microphone
- **Audio Output:** Built-in speaker

Video

- **Video Compression:** H.264
- **Frame Rate:** Configurable up to 30fps
- **Image Settings:**
  Full color
  Auto white/black balance and exposure
  Rotation: Mirror, Flip
  Configurable brightness, contrast, saturation
  Overlay capabilities: time, date, text

Alarm and Event Management

- **Input Trigger:** Motion/Sound detection
- **Notification Method:** E-mail, App notification, FTP
- **Detection Settings:**
  Configurable hot zone
  Adjustable sensitivity
  Store to Micro SD card
  Motion Tracking

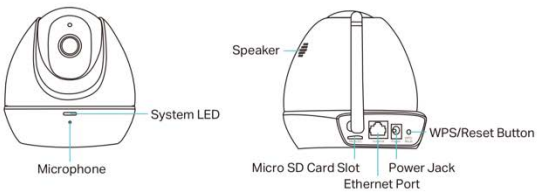
Network

- **Protocol:** Bonjour, TCP/IP, DHCP, ARP, ICMP, DNS, NTP, HTTP, HTTPS, TCP, UDP, ONVIF, RTSP, SMTP
- **Security:** Multiple password-protected user levels
- **Wireless Data Rates:** IEEE 802.11 b/g/n, up to 300Mbps
- **Frequency:** 2.4-2.4835GHz
- **Wireless Transmit Power:** <20dBm (EIRP)
- **Wireless Encryption:** WEP, WPA/WPA2, WPA-PSK/WPA2-PSK

Specifications

Hardware

- **Power Connector:** DC power jack
- **Ethernet:** RJ-45 for Ethernet 10/100 Base-T
- **Button:** WPS/Reset button
- **LED:** System LED, WPS LED
- **External Storage:** Micro SD card slot (Supports up to 128GB)
- **External Power Supply:** 12V/1A, Max 12W
- **Dimensions (W x D x H):** 5.7 x 4.3 x 4.2 in. (144 x 109 x 106 mm)



For more information, please visit
http://www.tp-link.com/en/products/details/?model=NC450
or scan the QR code left

Others

- **Certifications:** CE, FCC, RoHS
- **Package Contents**
  HD Pan&Tilt Day/Night Cloud Camera
  Passive PoE Injector
  Detachable Antenna
  Power Adapter
  Extension Cable
  RJ-45 Ethernet Cable
  Quick Installation Guide
  Ceiling/Wall Mount
- **System Requirements**
  Windows XP or higher, Mac OS X 10.7 or higher
  Android 4.1 or higher, iOS 7.0 or higher
- **Supported Browser**
  Microsoft Internet Explorer 8.0 or higher
  Firefox 4.0 or higher, Safari 5.0 or higher
  Chrome 5.0 or higher, Opera 12.0 or higher
- **Environment**
  Operating Temperature: 0°C~40°C (32°F ~104°F)
  Operating Humidity: 10%~90%RH, non-condensing

A.1.3 REOLINK RLC-420

RLC-420-5MP-IP-Camera-Specifications

	Model	RLC-420 (5MP)
Video	Image Sensor	1/2.7" CMOS Sensor
	Effective Pixels	2560x1920 (5.0 Megapixels)
	Lens	f=4.0mm F=2.0
	Angle of View	Horizontal: 80°, Vertical: 58°
	Day/Night Mode	Auto Switchover
	Min. Illumination	0 Lux (With IR Illuminator)
	IR Distance	IR Distance 30 Meters (LED: 18pcs/14mil/850nm)
	Backlight Compensation	Support
	Noise Reduction	3D DNR
	Compression	H.264
	Resolution	Main Stream: 2560x1920, 2560x1440, 2048x1536, 2304x1296; Sub Stream: 640x480
	Bitrate	Main Stream: 1024Kbps ~ 8192Kbps, Sub Stream: 64Kbps ~ 512Kbps
	Frame Rate	Main Stream@25fps, Sub Stream@6fps
Audio	Interface	Built-in Microphone
Network	Interface	One 10M/100Mbps RJ45
	Network Protocol	HTTPS, SSL, TCP/IP, UDP, UPNP, RTSP, SMTP, NTP, DHCP, DNS, DDNS, FTP, P2P
	Browser Supported	IE, Edge, Chrome, Firefox, Safari
	OS Supported	PC: Windows, Mac OS; Smart Phone: iOS, Android
	Max. User Access	20 Users (1 admin account & 19 user accounts); Support up to 12 simultaneous video streams (10 substreams & 2 mainstreams)
	Storage	Micro SD socket, support motion detect recording
General	Power Supply	DC12V & PoE (IEEE 802.3af)
	Power Consumption	<8W
	Working Environment	-10℃~+55℃(14°F~131°F), 10%~90%
	Ingress Protection	IP66
	Dimensions	Φ120*77mm
	Weight	480g

A.2 ΑΠΟΤΕΛΕΣΜΑΤΑ NMAP

A.2.1 FOSCAM R2

```
STARTING NMAP 7.70 ( HTTPS://NMAP.ORG ) AT 2019-05-01 09:34 EEST
NMAP SCAN REPORT FOR 192.168.2.11
HOST IS UP (0.00080S LATENCY).
NOT SHOWN: 65531 CLOSED PORTS
PORT     STATE SERVICE  VERSION
88/TCP   OPEN  HTTP     LIGHTTPD
443/TCP  OPEN  SSL/HTTP LIGHTTPD
888/TCP  OPEN  SOAP     GSOAP
65534/TCP OPEN  RTSP    D-LINK DCS-2130 OR PELCO IDE10DN WEBCAM RTSPD
MAC ADDRESS: 00:62:6E:82:43:CD (UNKNOWN)
SERVICE INFO: DEVICE: WEBCAM; CPE: CPE:/H:PELCO:IDE10DN

SERVICE DETECTION PERFORMED. PLEASE REPORT ANY INCORRECT RESULTS AT HTTPS://NMAP.ORG/SUBMIT/
.
NMAP DONE: 1 IP ADDRESS (1 HOST UP) SCANNED IN 43.19 SECONDS
STARTING NMAP 7.70 ( HTTPS://NMAP.ORG ) AT 2019-05-01 10:39 EEST
NMAP SCAN REPORT FOR 192.168.2.11
HOST IS UP (0.00066S LATENCY).
NOT SHOWN: 997 CLOSED PORTS
PORT    STATE SERVICE  VERSION
88/TCP  OPEN  HTTP     LIGHTTPD
443/TCP OPEN  SSL/HTTP LIGHTTPD
| SSL-CERT: SUBJECT: COMMONNAME=*.MYFOSCAM.ORG/ORGANIZATIONNAME=SHENZHEN FOSCAM
INTELLIGENT TECHNOLOGY CO.,LTD/STATEORPROVINCENAME=GUANGDONG/COUNTRYNAME=CN
| SUBJECT ALTERNATIVE NAME: DNS:*.MYFOSCAM.ORG, DNS:MYFOSCAM.ORG
| NOT VALID BEFORE: 2017-05-31T08:06:15
|_NOT VALID AFTER:  2020-05-29T08:06:15
888/TCP OPEN  SOAP     GSOAP
|_HTTP-SERVER-HEADER: GSOAP
|_HTTP-TITLE: SITE DOESN'T HAVE A TITLE (TEXT/XML; CHARSET=UTF-8).

SERVICE DETECTION PERFORMED. PLEASE REPORT ANY INCORRECT RESULTS AT HTTPS://NMAP.ORG/SUBMIT/
.
NMAP DONE: 1 IP ADDRESS (1 HOST UP) SCANNED IN 66.83 SECONDS
STARTING NMAP 7.70 ( HTTPS://NMAP.ORG ) AT 2019-05-01 10:41 EEST
NMAP SCAN REPORT FOR 192.168.2.11
HOST IS UP (0.00100S LATENCY).
NOT SHOWN: 997 CLOSED PORTS
PORT    STATE SERVICE  VERSION
88/TCP  OPEN  HTTP     LIGHTTPD
443/TCP OPEN  SSL/HTTP LIGHTTPD
888/TCP OPEN  SOAP     GSOAP

SERVICE DETECTION PERFORMED. PLEASE REPORT ANY INCORRECT RESULTS AT HTTPS://NMAP.ORG/SUBMIT/
.
NMAP DONE: 1 IP ADDRESS (1 HOST UP) SCANNED IN 24.65 SECONDS
STARTING NMAP 7.70 ( HTTPS://NMAP.ORG ) AT 2019-05-01 12:16 EEST
NMAP SCAN REPORT FOR 192.168.2.11
HOST IS UP (0.00077S LATENCY).
```

```
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
88/tcp  open  http     lighttpd
|_http-title: IPCam Client
443/tcp open  ssl/http lighttpd
| ssl-cert: Subject: commonName=*.myfoscam.org/organizationName=Shenzhen Foscam
Intelligent Technology Co.,Ltd/stateOrProvinceName=Guangdong/countryName=CN
| Subject Alternative Name: DNS:*.myfoscam.org, DNS:myfoscam.org
| Not valid before: 2017-05-31T08:06:15
|_Not valid after:  2020-05-29T08:06:15
888/tcp open  soap     gSOAP
|_http-server-header: gSOAP
|_http-title: Site doesn't have a title (text/xml; charset=utf-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 46.68 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-03 17:13 EEST
Nmap scan report for 192.168.2.11
Host is up (0.00061s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
88/tcp  open  kerberos-sec
443/tcp open  https
888/tcp open  accessbuilder
MAC Address: 00:62:6E:82:43:CD (Unknown)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=5/3%OT=88%CT=1%CU=32561%PV=Y%DS=1%DC=D%G=Y%M=0
0626E%TM
OS:=5CCC4C93%P=x86_64-apple-darwin13.4.0)SEQ(SP=102%GCD=1%ISR=106%TI=Z%CI=I
OS:%II=I%TS=U)OPS(O1=M550NNSNW4%O2=M550NNSNW4%O3=M550NW4%O4=M550NNS
NW4%O5=M
OS:550NNSNW4%O6=M550NNS)WIN(W1=3520%W2=3520%W3=3520%W4=3520%W5=352
0%W6=3520
OS:)ECN(R=Y%DF=Y%T=40%W=3520%O=M550NNSNW4%CC=Y%Q=)T1(R=Y%DF=Y%T=40
%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
RD=0%Q=)
OS:T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%
W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
=)U1(R=Y%D
OS:F=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
=N%T=4
OS:0%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.09 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-03 17:19 EEST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
```

```
|   224.0.0.251
|  After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.2.11
Host is up (0.00077s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
88/tcp  open  kerberos-sec
443/tcp open  https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.2.11
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.2.11:443/js/upfile.js?ver=
|     Form id: ' + formid + '
|_    Form action:
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
|_http-sql-injection: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
888/tcp open  accessbuilder
MAC Address: 00:62:6E:82:43:CD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 331.46 seconds
```

A.2.2 TP-LINK NC450

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-01 09:35 EEST
Nmap scan report for 192.168.2.16
Host is up (0.0019s latency).
Not shown: 65528 closed ports
PORT    STATE SERVICE       VERSION
80/tcp   open  http          lighttpd 1.4.32
443/tcp  open  ssl/http      lighttpd 1.4.32
554/tcp  open  rtsp          DoorBird video doorbell rtspd
2020/tcp open  soap          gSOAP 2.8
8080/tcp open  http-proxy    Streamd,A42BB014D915
8081/tcp open  blackice-icecap?
8088/tcp open  radan-http    VOD
3 services unrecognized despite returning data. If you know the service/version, please submit
the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.70%I=7%D=5/1%Time=5CC93E37%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,15D,"HTTP/1\.0\x20401\x20Unauthorized\r\nServer:\x20Strea
SF:md,A42BB014D915\r\nDate:\x20Wed,\x2001\x20May\x202019\x2006:35:34\x20UT
SF:C\r\nPragma:\x20no-cache\r\nCache-Control:\x20no-cache\r\nContent-Lengt
SF:h:\x200\r\nWWW-Authenticate:\x20Digest\x20realm=\"TP-Link\x20IP-Camera\
SF:",algorithm=\"MD5\",qop=\"auth\",nonce=\"ba858619fb77b3171e76938d7f9cce
SF:9800001dce14e5e604\",opaque=\"6494321465464984656564621\"\r\nConnectio
```

SF:n:\x20close\r\n\r\n")%r(HTTPOptions,15D,"HTTP/1\.0\x20401\x20Unauthoriz
SF:ed\r\nServer:\x20Streamd,A42BB014D915\r\nDate:\x20Wed,\x2001\x20May\x20
SF:2019\x2006:35:34\x20UTC\r\nPragma:\x20no-cache\r\nCache-Control:\x20no-
SF:cache\r\nContent-Length:\x200\r\nWWW-Authenticate:\x20Digest\x20realm=\
SF:"TP-Link\x20IP-Camera\",algorithm=\"MD5\",qop=\"auth\",nonce=\"38864a59
SF:fb157693b5a47511b759495600001dce16551b23\",opaque=\"6494321465464984656
SF:5646421\"\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,10C,"HTTP/1\.
SF:0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r\nDate:\
SF:x20Wed,\x2001\x20May\x202019\x2006:35:34\x20UTC\r\nContent-Type:\x20tex
SF:t/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\n<!DOCTY
SF:PE\x20HTML><html><head><title>400\x20Bad\x20Request</title></head><body
SF:><h1>400\x20Bad\x20Request</h1></body></html>")%r(FourOhFourRequest,106
SF:,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Streamd,A42BB014D915\r
SF:\nDate:\x20Wed,\x2001\x20May\x202019\x2006:35:34\x20UTC\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\
SF:n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head
SF:><body><h1>404\x20Not\x20Found</h1></body></html>")%r(Socks5,10C,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r\nDat
SF:e:\x20Wed,\x2001\x20May\x202019\x2006:35:34\x20UTC\r\nContent-Type:\x20
SF:text/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\n<!DO
SF:CTYPE\x20HTML><html><head><title>400\x20Bad\x20Request</title></head><b
SF:ody><h1>400\x20Bad\x20Request</h1></body></html>")%r(GenericLines,10C,"
SF:HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r
SF:\nDate:\x20Wed,\x2001\x20May\x202019\x2006:35:39\x20UTC\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\
SF:n<!DOCTYPE\x20HTML><html><head><title>400\x20Bad\x20Request</title></he
SF:ad><body><h1>400\x20Bad\x20Request</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8081-TCP:V=7.70%I=7%D=5/1%Time=5CC93E37%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,F9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Speake
SF:r\r\nDate:\x20Wed,\x2001\x20May\x202019\x2006:35:34\x20UTC\r\nContent-T
SF:ype:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n
SF:\r\n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></h
SF:ead><body><h1>404\x20Not\x20Found</h1></body></html>")%r(FourOhFourRequ
SF:est,F9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Speaker\r\nDate:
SF:\x20Wed,\x2001\x20May\x202019\x2006:35:34\x20UTC\r\nContent-Type:\x20te
SF:xt/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCT
SF:YPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head><body>
SF:<h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F9,"HTTP/1\.
SF:0\x20404\x20Not\x20Found\r\nServer:\x20Speaker\r\nDate:\x20Wed,\x2001\x
SF:20May\x202019\x2006:35:39\x20UTC\r\nContent-Type:\x20text/html\r\nConte
SF:nt-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><htm
SF:l><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x
SF:20Found</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8088-TCP:V=7.70%I=7%D=5/1%Time=5CC93E37%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,F5,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\
SF:nDate:\x20Wed,\x2001\x20May\x202019\x2006:35:34\x20UTC\r\nContent-Type:
SF:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n
SF:<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head>
SF:<body><h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F5,"HT
SF:TP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001
SF:\x20May\x202019\x2006:35:39\x20UTC\r\nContent-Type:\x20text/html\r\nCon
SF:tent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><h
SF:tml><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not
SF:\x20Found</h1></body></html>")%r(FourOhFourRequest,F5,"HTTP/1\.0\x20404

SF:\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001\x20May\x20201
SF:9\x2006:36:26\x20UTC\r\nContent-Type:\x20text/html\r\nContent-Length:\x
SF:20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><html><head><tit
SF:le>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x20Found</h1>
SF:</body></html>");
MAC Address: A4:2B:B0:14:D9:15 (Tp-link Technologies)
Service Info: Device: webcam

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 138.72 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-01 10:40 EEST
Nmap scan report for 192.168.2.16
Host is up (0.00066s latency).
Not shown: 993 closed ports
PORT   STATE SERVICE   VERSION
80/tcp open http   lighttpd 1.4.32
|_http-server-header: lighttpd/1.4.32
|_http-title: Site doesn't have a title (text/html).
443/tcp open ssl/http   lighttpd 1.4.32
|_http-server-header: lighttpd/1.4.32
|_http-title: NC450 Admin - Login
| ssl-cert: Subject:
commonName=localhost/stateOrProvinceName=Guangdong/countryName=CN
| Not valid before: 2019-05-01T04:28:11
|_Not valid after: 2029-03-09T04:28:11
|_ssl-date: 2019-05-01T07:42:21+00:00; -1s from scanner time.
554/tcp open rtsp   DoorBird video doorbell rtspd
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER,
SET_PARAMETER
2020/tcp open soap   gSOAP 2.8
|_http-server-header: gSOAP/2.8
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
8080/tcp open http-proxy   Streamd,A42BB014D915
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 404 Not Found
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 07:40:22 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404
Not Found</h1></body></html>
| GenericLines:
| HTTP/1.0 400 Bad Request
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 07:40:27 UTC
| Content-Type: text/html
| Content-Length: 108
| Connection: close
| <!DOCTYPE HTML><html><head><title>400 Bad Request</title></head><body><h1>400
Bad Request</h1></body></html>
| GetRequest:
| HTTP/1.0 401 Unauthorized
| Server: Streamd,A42BB014D915

| Date: Wed, 01 May 2019 07:40:22 UTC
| Pragma: no-cache
| Cache-Control: no-cache
| Content-Length: 0
| WWW-Authenticate: Digest realm="TP-Link IP-Camera",algorithm="MD5",qop="auth",nonce="2a817a9fe256f714b2aa30056c55bfc200002cfe362509c5",opaque="6494321465464984656564642 1"
| Connection: close
| HTTPOptions:
| HTTP/1.0 401 Unauthorized
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 07:40:22 UTC
| Pragma: no-cache
| Cache-Control: no-cache
| Content-Length: 0
| WWW-Authenticate: Digest realm="TP-Link IP-Camera",algorithm="MD5",qop="auth",nonce="0ef8f3c09595b1b33d210f0eadff46c000002cfe36ada56e",opaque="6494321465464984656564642 1"
| Connection: close
| RTSPRequest, Socks5:
| HTTP/1.0 400 Bad Request
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 07:40:22 UTC
| Content-Type: text/html
| Content-Length: 108
| Connection: close
|_ <!DOCTYPE HTML><html><head><title>400 Bad Request</title></head><body><h1>400 Bad Request</h1></body></html>
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_ Digest realm=TP-Link IP-Camera nonce=b0f0a34bb887712cae856653fd0ffee500002d771295d78b opaque=6494321465464984656564642 1 qop=auth algorithm=MD5
|_http-server-header: Streamd,A42BB014D915
|_http-title: Site doesn't have a title.
8081/tcp open blackice-icecap?
| fingerprint-strings:
| FourOhFourRequest, GetRequest:
| HTTP/1.0 404 Not Found
| Server: Speaker
| Date: Wed, 01 May 2019 07:40:22 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
| HTTPOptions:
| HTTP/1.0 404 Not Found
| Server: Speaker
| Date: Wed, 01 May 2019 07:40:27 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
|_ <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
8088/tcp open radan-http vod

| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 404 Not Found
| Server: vod
| Date: Wed, 01 May 2019 07:41:15 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
| GetRequest:
| HTTP/1.0 404 Not Found
| Server: vod
| Date: Wed, 01 May 2019 07:40:22 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
| HTTPOptions:
| HTTP/1.0 404 Not Found
| Server: vod
| Date: Wed, 01 May 2019 07:40:27 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
|_ <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
|_http-server-header: vod
|_http-title: 404 Not Found
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.70%I=7%D=5/1%Time=5CC94D67%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,15D,"HTTP/1\.0\x20401\x20Unauthorized\r\nServer:\x20Strea
SF:md,A42BB014D915\r\nDate:\x20Wed,\x2001\x20May\x202019\x2007:40:22\x20UT
SF:C\r\nPragma:\x20no-cache\r\nCache-Control:\x20no-cache\r\nContent-Lengt
SF:h:\x200\r\nWWW-Authenticate:\x20Digest\x20realm=\"TP-Link\x20IP-Camera\
SF:",algorithm=\"MD5\",qop=\"auth\",nonce=\"2a817a9fe256f714b2aa30056c55bf
SF:c200002cfe362509c5\",opaque=\"6494321465464984656565646421\"\r\nConnectio
SF:n:\x20close\r\n\r\n")%r(HTTPOptions,15D,"HTTP/1\.0\x20401\x20Unauthoriz
SF:ed\r\nServer:\x20Streamd,A42BB014D915\r\nDate:\x20Wed,\x2001\x20May\x20
SF:2019\x2007:40:22\x20UTC\r\nPragma:\x20no-cache\r\nCache-Control:\x20no-
SF:cache\r\nContent-Length:\x200\r\nWWW-Authenticate:\x20Digest\x20realm=\
SF:"TP-Link\x20IP-Camera\",algorithm=\"MD5\",qop=\"auth\",nonce=\"0ef8f3c0
SF:9595b1b33d210f0eadff46c000002cfe36ada56e\",opaque=\"6494321465464984656
SF:5646421\"\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,10C,"HTTP/1\.
SF:0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r\nDate:\
SF:x20Wed,\x2001\x20May\x202019\x2007:40:22\x20UTC\r\nContent-Type:\x20tex
SF:t/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\n<!DOCTY
SF:PE\x20HTML><html><head><title>400\x20Bad\x20Request</title></head><body
SF:><h1>400\x20Bad\x20Request</h1></body></html>")%r(FourOhFourRequest,106
SF:,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Streamd,A42BB014D915\r
SF:\nDate:\x20Wed,\x2001\x20May\x202019\x2007:40:22\x20UTC\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\
SF:n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head

SF:><body><h1>404\x20Not\x20Found</h1></body></html>")%r(Socks5,10C,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r\nDat
SF:e:\x20Wed,\x2001\x20May\x202019\x2007:40:22\x20UTC\r\nContent-Type:\x20
SF:text/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\n<!DO
SF:CTYPE\x20HTML><html><head><title>400\x20Bad\x20Request</title></head><b
SF:ody><h1>400\x20Bad\x20Request</h1></body></html>")%r(GenericLines,10C,"
SF:HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r
SF:\nDate:\x20Wed,\x2001\x20May\x202019\x2007:40:27\x20UTC\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\
SF:n<!DOCTYPE\x20HTML><html><head><title>400\x20Bad\x20Request</title></he
SF:ad><body><h1>400\x20Bad\x20Request</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8081-TCP:V=7.70%I=7%D=5/1%Time=5CC94D67%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,F9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Speake
SF:r\r\nDate:\x20Wed,\x2001\x20May\x202019\x2007:40:22\x20UTC\r\nContent-T
SF:ype:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n
SF:\r\n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></h
SF:ead><body><h1>404\x20Not\x20Found</h1></body></html>")%r(FourOhFourRequ
SF:est,F9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Speaker\r\nDate:
SF:\x20Wed,\x2001\x20May\x202019\x2007:40:22\x20UTC\r\nContent-Type:\x20te
SF:xt/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCT
SF:YPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head><body>
SF:<h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F9,"HTTP/1\.
SF:0\x20404\x20Not\x20Found\r\nServer:\x20Speaker\r\nDate:\x20Wed,\x2001\x
SF:20May\x202019\x2007:40:27\x20UTC\r\nContent-Type:\x20text/html\r\nConte
SF:nt-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><htm
SF:l><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x
SF:20Found</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8088-TCP:V=7.70%I=7%D=5/1%Time=5CC94D67%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,F5,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\
SF:nDate:\x20Wed,\x2001\x20May\x202019\x2007:40:22\x20UTC\r\nContent-Type:
SF:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n
SF:<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head>
SF:<body><h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F5,"HT
SF:TP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001
SF:\x20May\x202019\x2007:40:27\x20UTC\r\nContent-Type:\x20text/html\r\nCon
SF:tent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><h
SF:tml><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not
SF:\x20Found</h1></body></html>")%r(FourOhFourRequest,F5,"HTTP/1\.0\x20404
SF:\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001\x20May\x20201
SF:9\x2007:41:15\x20UTC\r\nContent-Type:\x20text/html\r\nContent-Length:\x
SF:20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><html><head><tit
SF:le>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x20Found</h1>
SF:</body></html>");
Service Info: Device: webcam

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 135.32 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-01 10:43 EEST
Nmap scan report for 192.168.2.16
Host is up (0.00066s latency).

```
NOT SHOWN: 993 CLOSED PORTS
PORT    STATE SERVICE       VERSION
80/TCP   OPEN  HTTP          LIGHTTPD 1.4.32
443/TCP  OPEN  SSL/HTTP      LIGHTTPD 1.4.32
554/TCP  OPEN  RTSP          DOORBIRD VIDEO DOORBELL RTSPD
2020/TCP OPEN  SOAP          GSOAP 2.8
8080/TCP OPEN  HTTP-PROXY    STREAMD,A42BB014D915
8081/TCP OPEN  BLACKICE-ICECAP?
8088/TCP OPEN  RADAN-HTTP    VOD
3 SERVICES UNRECOGNIZED DESPITE RETURNING DATA. IF YOU KNOW THE SERVICE/VERSION, PLEASE SUBMIT
THE FOLLOWING FINGERPRINTS AT HTTPS://NMAP.ORG/CGI-BIN/SUBMIT.CGI?NEW-SERVICE :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-PORT8080-TCP:V=7.70%I=9%D=5/1%TIME=5CC94E22%P=X86_64-APPLE-DARWIN13.4.0
SF:%R(GETREQUEST,15D,"HTTP/1\.0\X20401\X20UNAUTHORIZED\R\NSERVER:\X20STREA
SF:MD,A42BB014D915\R\NDATE:\X20WED,\X2001\X20MAY\X202019\X2007:43:29\X20UT
SF:C\R\NPRAGMA:\X20NO-CACHE\R\NCACHE-CONTROL:\X20NO-CACHE\R\NCONTENT-LENGT
SF:H:\X200\R\NWWW-AUTHENTICATE:\X20DIGEST\X20REALM=\"TP-LINK\X20IP-CAMERA\
SF:",ALGORITHM=\"MD5\",QOP=\"AUTH\",NONCE=\"EA7A3EB02DAD2A1F7EBEBA581BF1A1
SF:3E00002DB9398B1CCE\",OPAQUE=\"64943214654649846565646421\"\R\NCONNECTIO
SF:N:\X20CLOSE\R\N\R\N")%R(HTTPOPTIONS,15D,"HTTP/1\.0\X20401\X20UNAUTHORIZ
SF:ED\R\NSERVER:\X20STREAMD,A42BB014D915\R\NDATE:\X20WED,\X2001\X20MAY\X20
SF:2019\X2007:43:29\X20UTC\R\NPRAGMA:\X20NO-CACHE\R\NCACHE-CONTROL:\X20NO-
SF:CACHE\R\NCONTENT-LENGTH:\X200\R\NWWW-AUTHENTICATE:\X20DIGEST\X20REALM=\
SF:"TP-LINK\X20IP-CAMERA\",ALGORITHM=\"MD5\",QOP=\"AUTH\",NONCE=\"0448370C
SF:E467BD5C2D1D300D764A5BB400002DB93B06BDF3\",OPAQUE=\"6494321465464984656
SF:5646421\"\R\NCONNECTION:\X20CLOSE\R\N\R\N")%R(RTSPREQUEST,10C,"HTTP/1\.
SF:0\X20400\X20BAD\X20REQUEST\R\NSERVER:\X20STREAMD,A42BB014D915\R\NDATE:\
SF:X20WED,\X2001\X20MAY\X202019\X2007:43:29\X20UTC\R\NCONTENT-TYPE:\X20TEX
SF:T/HTML\R\NCONTENT-LENGTH:\X20108\R\NCONNECTION:\X20CLOSE\R\N\R\N<!DOCTY
SF:PE\X20HTML><HTML><HEAD><TITLE>400\X20BAD\X20REQUEST</TITLE></HEAD><BODY
SF:><H1>400\X20BAD\X20REQUEST</H1></BODY></HTML>")%R(FOUROHFOURREQUEST,106
SF:,"HTTP/1\.0\X20404\X20NOT\X20FOUND\R\NSERVER:\X20STREAMD,A42BB014D915\R
SF:\NDATE:\X20WED,\X2001\X20MAY\X202019\X2007:43:29\X20UTC\R\NCONTENT-TYPE
SF::\X20TEXT/HTML\R\NCONTENT-LENGTH:\X20104\R\NCONNECTION:\X20CLOSE\R\N\R\
SF:N<!DOCTYPE\X20HTML><HTML><HEAD><TITLE>404\X20NOT\X20FOUND</TITLE></HEAD
SF:><BODY><H1>404\X20NOT\X20FOUND</H1></BODY></HTML>")%R(SOCKS5,10C,"HTTP/
SF:1\.0\X20400\X20BAD\X20REQUEST\R\NSERVER:\X20STREAMD,A42BB014D915\R\NDAT
SF:E:\X20WED,\X2001\X20MAY\X202019\X2007:43:29\X20UTC\R\NCONTENT-TYPE:\X20
SF:TEXT/HTML\R\NCONTENT-LENGTH:\X20108\R\NCONNECTION:\X20CLOSE\R\N\R\N<!DO
SF:CTYPE\X20HTML><HTML><HEAD><TITLE>400\X20BAD\X20REQUEST</TITLE></HEAD><B
SF:ODY><H1>400\X20BAD\X20REQUEST</H1></BODY></HTML>")%R(GENERICLINES,10C,"
SF:HTTP/1\.0\X20400\X20BAD\X20REQUEST\R\NSERVER:\X20STREAMD,A42BB014D915\R
SF:\NDATE:\X20WED,\X2001\X20MAY\X202019\X2007:43:34\X20UTC\R\NCONTENT-TYPE
SF::\X20TEXT/HTML\R\NCONTENT-LENGTH:\X20108\R\NCONNECTION:\X20CLOSE\R\N\R\
SF:N<!DOCTYPE\X20HTML><HTML><HEAD><TITLE>400\X20BAD\X20REQUEST</TITLE></HE
SF:AD><BODY><H1>400\X20BAD\X20REQUEST</H1></BODY></HTML>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-PORT8081-TCP:V=7.70%I=9%D=5/1%TIME=5CC94E22%P=X86_64-APPLE-DARWIN13.4.0
SF:%R(GETREQUEST,F9,"HTTP/1\.0\X20404\X20NOT\X20FOUND\R\NSERVER:\X20SPEAKE
SF:R\R\NDATE:\X20WED,\X2001\X20MAY\X202019\X2007:43:29\X20UTC\R\NCONTENT-T
SF:YPE:\X20TEXT/HTML\R\NCONTENT-LENGTH:\X20104\R\NCONNECTION:\X20CLOSE\R\N
SF:\R\N<!DOCTYPE\X20HTML><HTML><HEAD><TITLE>404\X20NOT\X20FOUND</TITLE></H
SF:EAD><BODY><H1>404\X20NOT\X20FOUND</H1></BODY></HTML>")%R(FOUROHFOURREQU
SF:EST,F9,"HTTP/1\.0\X20404\X20NOT\X20FOUND\R\NSERVER:\X20SPEAKER\R\NDATE:
SF:\X20WED,\X2001\X20MAY\X202019\X2007:43:29\X20UTC\R\NCONTENT-TYPE:\X20TE
SF:XT/HTML\R\NCONTENT-LENGTH:\X20104\R\NCONNECTION:\X20CLOSE\R\N\R\N<!DOCT
```

SF:YPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head><body>
SF:<h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F9,"HTTP/1\.
SF:0\x20404\x20Not\x20Found\r\nServer:\x20Speaker\r\nDate:\x20Wed,\x2001\x
SF:20May\x202019\x2007:43:34\x20UTC\r\nContent-Type:\x20text/html\r\nConte
SF:nt-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><htm
SF:l><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x
SF:20Found</h1></body></html>")%r(OfficeScan,F9,"HTTP/1\.0\x20404\x20Not\x
SF:20Found\r\nServer:\x20Speaker\r\nDate:\x20Wed,\x2001\x20May\x202019\x20
SF:07:46:19\x20UTC\r\nContent-Type:\x20text/html\r\nContent-Length:\x20104
SF:\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><html><head><title>40
SF:4\x20Not\x20Found</title></head><body><h1>404\x20Not\x20Found</h1></bod
SF:y></html>")%r(apple-iphoto,F9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServ
SF:er:\x20Speaker\r\nDate:\x20Wed,\x2001\x20May\x202019\x2007:47:50\x20UTC
SF:\r\nContent-Type:\x20text/html\r\nContent-Length:\x20104\r\nConnection:
SF:\x20close\r\n\r\n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Fou
SF:nd</title></head><body><h1>404\x20Not\x20Found</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8088-TCP:V=7.70%I=9%D=5/1%Time=5CC94E22%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,F5,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\
SF:nDate:\x20Wed,\x2001\x20May\x202019\x2007:43:29\x20UTC\r\nContent-Type:
SF:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n
SF:<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head>
SF:<body><h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F5,"HT
SF:TP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001
SF:\x20May\x202019\x2007:43:34\x20UTC\r\nContent-Type:\x20text/html\r\nCon
SF:tent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><h
SF:tml><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not
SF:\x20Found</h1></body></html>")%r(FourOhFourRequest,F5,"HTTP/1\.0\x20404
SF:\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001\x20May\x20201
SF:9\x2007:44:34\x20UTC\r\nContent-Type:\x20text/html\r\nContent-Length:\x
SF:20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><html><head><tit
SF:le>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x20Found</h1>
SF:</body></html>")%r(OfficeScan,F5,"HTTP/1\.0\x20404\x20Not\x20Found\r\nS
SF:erver:\x20vod\r\nDate:\x20Wed,\x2001\x20May\x202019\x2007:46:19\x20UTC\
SF:r\nContent-Type:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\
SF:x20close\r\n\r\n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Foun
SF:d</title></head><body><h1>404\x20Not\x20Found</h1></body></html>")%r(ap
SF:ple-iphoto,F5,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\nDa
SF:te:\x20Wed,\x2001\x20May\x202019\x2007:47:50\x20UTC\r\nContent-Type:\x2
SF:0text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!D
SF:OCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head><bo
SF:dy><h1>404\x20Not\x20Found</h1></body></html>");
Service Info: Device: webcam

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 5028.70 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-01 12:17 EEST
Nmap scan report for 192.168.2.16
Host is up (0.00042s latency).
Not shown: 993 closed ports
PORT   STATE SERVICE   VERSION
80/tcp open http   lighttpd 1.4.32
|_http-server-header: lighttpd/1.4.32
|_http-title: Site doesn't have a title (text/html).
443/tcp open ssl/http   lighttpd 1.4.32

|_http-server-header: lighttpd/1.4.32
|_http-title: NC450 Admin - Login
| ssl-cert: Subject:
commonName=localhost/stateOrProvinceName=Guangdong/countryName=CN
| Not valid before: 2019-05-01T04:28:11
|_Not valid after: 2029-03-09T04:28:11
|_ssl-date: 2019-05-01T09:19:15+00:00; -1s from scanner time.
554/tcp open rtsp   DoorBird video doorbell rtspd
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER,
SET_PARAMETER
2020/tcp open soap   gSOAP 2.8
|_http-server-header: gSOAP/2.8
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
8080/tcp open http-proxy   Streamd,A42BB014D915
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 404 Not Found
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 09:17:15 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404
Not Found</h1></body></html>
| GenericLines:
| HTTP/1.0 400 Bad Request
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 09:17:20 UTC
| Content-Type: text/html
| Content-Length: 108
| Connection: close
| <!DOCTYPE HTML><html><head><title>400 Bad Request</title></head><body><h1>400
Bad Request</h1></body></html>
| GetRequest:
| HTTP/1.0 401 Unauthorized
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 09:17:15 UTC
| Pragma: no-cache
| Cache-Control: no-cache
| Content-Length: 0
| WWW-Authenticate: Digest realm="TP-Link IP-
Camera",algorithm="MD5",qop="auth",nonce="2f5d679313839630bfb7a9182a1a506b000043
b400bcf9e6",opaque="6494321465464984656564642l"
| Connection: close
| HTTPOptions:
| HTTP/1.0 401 Unauthorized
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 09:17:15 UTC
| Pragma: no-cache
| Cache-Control: no-cache
| Content-Length: 0
| WWW-Authenticate: Digest realm="TP-Link IP-
Camera",algorithm="MD5",qop="auth",nonce="bf2266afba641da403c8bcea50e00a0f000043b
401e10a61",opaque="6494321465464984656564642l"
| Connection: close
| RTSPRequest, Socks5:

| HTTP/1.0 400 Bad Request
| Server: Streamd,A42BB014D915
| Date: Wed, 01 May 2019 09:17:15 UTC
| Content-Type: text/html
| Content-Length: 108
| Connection: close
|_ <!DOCTYPE HTML><html><head><title>400 Bad Request</title></head><body><h1>400 Bad Request</h1></body></html>
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_ Digest realm=TP-Link IP-Camera nonce=0d5fcc6ac5d7ab1e19e9c3f7013743f5000044293ace9071 qop=auth opaque=649432146546498465646421 algorithm=MD5
|_http-server-header: Streamd,A42BB014D915
|_http-title: Site doesn't have a title.
8081/tcp open blackice-icecap?
| fingerprint-strings:
| FourOhFourRequest, GetRequest:
| HTTP/1.0 404 Not Found
| Server: Speaker
| Date: Wed, 01 May 2019 09:17:15 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
| HTTPOptions:
| HTTP/1.0 404 Not Found
| Server: Speaker
| Date: Wed, 01 May 2019 09:17:20 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
|_ <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
8088/tcp open radan-http vod
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 404 Not Found
| Server: vod
| Date: Wed, 01 May 2019 09:18:08 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
| GetRequest:
| HTTP/1.0 404 Not Found
| Server: vod
| Date: Wed, 01 May 2019 09:17:15 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
| <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
| HTTPOptions:

| HTTP/1.0 404 Not Found
| Server: vod
| Date: Wed, 01 May 2019 09:17:20 UTC
| Content-Type: text/html
| Content-Length: 104
| Connection: close
|_ <!DOCTYPE HTML><html><head><title>404 Not Found</title></head><body><h1>404 Not Found</h1></body></html>
|_http-server-header: vod
|_http-title: 404 Not Found
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.70%I=7%D=5/1%Time=5CC9641D%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,15D,"HTTP/1\.0\x20401\x20Unauthorized\r\nServer:\x20Strea
SF:md,A42BB014D915\r\nDate:\x20Wed,\x2001\x20May\x202019\x2009:17:15\x20UT
SF:C\r\nPragma:\x20no-cache\r\nCache-Control:\x20no-cache\r\nContent-Lengt
SF:h:\x200\r\nWWW-Authenticate:\x20Digest\x20realm=\"TP-Link\x20IP-Camera\
SF:",algorithm=\"MD5\",qop=\"auth\",nonce=\"2f5d679313839630bfb7a9182a1a50
SF:6b000043b400bcf9e6\",opaque=\"6494321465464984656565646421\"\r\nConnectio
SF:n:\x20close\r\n\r\n")%r(HTTPOptions,15D,"HTTP/1\.0\x20401\x20Unauthoriz
SF:ed\r\nServer:\x20Streamd,A42BB014D915\r\nDate:\x20Wed,\x2001\x20May\x20
SF:2019\x2009:17:15\x20UTC\r\nPragma:\x20no-cache\r\nCache-Control:\x20no-
SF:cache\r\nContent-Length:\x200\r\nWWW-Authenticate:\x20Digest\x20realm=\
SF:"TP-Link\x20IP-Camera\",algorithm=\"MD5\",qop=\"auth\",nonce=\"bf2266af
SF:ba641da403c8bcea50e00a0f000043b401e10a61\",opaque=\"6494321465464984656
SF:5646421\"\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,10C,"HTTP/1\.
SF:0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r\nDate:\
SF:x20Wed,\x2001\x20May\x202019\x2009:17:15\x20UTC\r\nContent-Type:\x20tex
SF:t/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\n<!DOCTY
SF:PE\x20HTML><html><head><title>400\x20Bad\x20Request</title></head><body
SF:><h1>400\x20Bad\x20Request</h1></body></html>")%r(FourOhFourRequest,106
SF:,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Streamd,A42BB014D915\r
SF:\nDate:\x20Wed,\x2001\x20May\x202019\x2009:17:15\x20UTC\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\
SF:n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head
SF:><body><h1>404\x20Not\x20Found</h1></body></html>")%r(Socks5,10C,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r\nDat
SF:e:\x20Wed,\x2001\x20May\x202019\x2009:17:15\x20UTC\r\nContent-Type:\x20
SF:text/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\n<!DO
SF:CTYPE\x20HTML><html><head><title>400\x20Bad\x20Request</title></head><b
SF:ody><h1>400\x20Bad\x20Request</h1></body></html>")%r(GenericLines,10C,"
SF:HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20Streamd,A42BB014D915\r
SF:\nDate:\x20Wed,\x2001\x20May\x202019\x2009:17:20\x20UTC\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20108\r\nConnection:\x20close\r\n\r\
SF:n<!DOCTYPE\x20HTML><html><head><title>400\x20Bad\x20Request</title></he
SF:ad><body><h1>400\x20Bad\x20Request</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8081-TCP:V=7.70%I=7%D=5/1%Time=5CC9641D%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,F9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Speake
SF:r\r\nDate:\x20Wed,\x2001\x20May\x202019\x2009:17:15\x20UTC\r\nContent-T
SF:ype:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n
SF:\r\n<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></h
SF:ead><body><h1>404\x20Not\x20Found</h1></body></html>")%r(FourOhFourRequ
SF:est,F9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20Speaker\r\nDate:
SF:\x20Wed,\x2001\x20May\x202019\x2009:17:15\x20UTC\r\nContent-Type:\x20te

SF:xt/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCT
SF:YPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head><body>
SF:<h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F9,"HTTP/1\.
SF:0\x20404\x20Not\x20Found\r\nServer:\x20Speaker\r\nDate:\x20Wed,\x2001\x
SF:20May\x202019\x2009:17:20\x20UTC\r\nContent-Type:\x20text/html\r\nConte
SF:nt-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><htm
SF:l><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x
SF:20Found</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8088-TCP:V=7.70%I=7%D=5/1%Time=5CC9641D%P=x86_64-apple-darwin13.4.0
SF:%r(GetRequest,F5,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\
SF:nDate:\x20Wed,\x2001\x20May\x202019\x2009:17:15\x20UTC\r\nContent-Type:
SF:\x20text/html\r\nContent-Length:\x20104\r\nConnection:\x20close\r\n\r\n
SF:<!DOCTYPE\x20HTML><html><head><title>404\x20Not\x20Found</title></head>
SF:<body><h1>404\x20Not\x20Found</h1></body></html>")%r(HTTPOptions,F5,"HT
SF:TP/1\.0\x20404\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001
SF:\x20May\x202019\x2009:17:20\x20UTC\r\nContent-Type:\x20text/html\r\nCon
SF:tent-Length:\x20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><h
SF:tml><head><title>404\x20Not\x20Found</title></head><body><h1>404\x20Not
SF:\x20Found</h1></body></html>")%r(FourOhFourRequest,F5,"HTTP/1\.0\x20404
SF:\x20Not\x20Found\r\nServer:\x20vod\r\nDate:\x20Wed,\x2001\x20May\x20201
SF:9\x2009:18:08\x20UTC\r\nContent-Type:\x20text/html\r\nContent-Length:\x
SF:20104\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML><html><head><tit
SF:le>404\x20Not\x20Found</title></head><body><h1>404\x20Not\x20Found</h1>
SF:</body></html>");
Service Info: Device: webcam

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 134.29 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-03 17:19 EEST
Nmap scan report for 192.168.2.16
Host is up (0.00084s latency).
Not shown: 993 closed ports
PORT   STATE SERVICE
80/tcp open http
443/tcp open https
554/tcp open rtsp
2020/tcp open xinupageserver
8080/tcp open http-proxy
8081/tcp open blackice-icecap
8088/tcp open radan-http
MAC Address: A4:2B:B0:14:D9:15 (Tp-link Technologies)
Device type: WAP
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.26
OS details: OpenWrt Kamikaze 8.09 (Linux 2.6.26)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.12 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-03 17:25 EEST
Pre-scan script results:

| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.2.16
Host is up (0.0011s latency).
Not shown: 993 filtered ports
PORT STATE SERVICE
80/tcp open http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /globalSIPsettings.html: Aastra IP Phone
| /SIPsettingsLine1.html: Aastra IP Phone
| //system.html: CMNC-200 IP Camera
| /siteadmin/login.html: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin_area/login.html: Possible admin folder
| /admin_area/index.html: Possible admin folder
| /admincp/index.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /adminpanel.html: Possible admin folder
| /webadmin.html: Possible admin folder
| /webadmin/index.html: Possible admin folder
| /webadmin/admin.html: Possible admin folder
| /webadmin/login.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin_login.html: Possible admin folder
| /panel-administracion/login.html: Possible admin folder
| /admin_area/admin.html: Possible admin folder
| /bb-admin/index.html: Possible admin folder
| /bb-admin/login.html: Possible admin folder
| /bb-admin/admin.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /pages/admin/admin-login.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin-login.html: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /adminLogin.html: Possible admin folder
| /home.html: Possible admin folder
| /adminarea/index.html: Possible admin folder
| /adminarea/admin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /cp.html: Possible admin folder
| /moderator.html: Possible admin folder
| /administrator/index.html: Possible admin folder
| /administrator/login.html: Possible admin folder
| /user.html: Possible admin folder
| /administrator/account.html: Possible admin folder
| /administrator.html: Possible admin folder
| /login.html: Possible admin folder

| /modelsearch/login.html: Possible admin folder
| /moderator/login.html: Possible admin folder
| /adminarea/login.html: Possible admin folder
| /panel-administracion/index.html: Possible admin folder
| /panel-administracion/admin.html: Possible admin folder
| /modelsearch/index.html: Possible admin folder
| /modelsearch/admin.html: Possible admin folder
| /admincontrol/login.html: Possible admin folder
| /adm/index.html: Possible admin folder
| /adm.html: Possible admin folder
| /moderator/admin.html: Possible admin folder
| /account.html: Possible admin folder
| /controlpanel.html: Possible admin folder
| /admincontrol.html: Possible admin folder
| /test.html: Test page
| /TopToolArea.html: Alteon OS BBI (Nortell)
| /switchSystem.html: Alteon OS BBI (Nortell)
| /test/logon.html: Jetty
| /setup/password_required.html: 2WIRE GATEWAY
| /CFIDE/Administrator/startstop.html: ColdFusion Admin Console
| /HW_logo.html: Huawei HG 530
| /postinfo.html: Frontpage file or folder
| /readme.html: Interesting, a readme.
| /pligg/readme.html: Interesting, a readme.
| /digg/readme.html: Interesting, a readme.
| /news/readme.html: Interesting, a readme.
| /tinymcpuk/filemanager/browser.html: CMS Lokomedia
| /scripts/fckeditor/editor/filemanager/connectors/test.html: Digitalus CMS/FCKEditor File upload
| /scripts/fckeditor/editor/filemanager/connectors/uploadtest.html: Digitalus CMS/FCKEditor File upload
| /fckeditor/editor/filemanager/connectors/test.html: phpmotion/FCKEditor File upload
| /fckeditor/editor/filemanager/upload/test.html: Geeklog/FCKEditor File upload
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKEditor File upload
| /FCKEditor/editor/filemanager/browser/default/connectors/test.html: EgO or osCMax/FCKEditor File upload
| /_plugin/fckeditor/editor/filemanager/connectors/test.html: SweetRice/FCKEditor File upload
| /fckeditor/editor/filemanager/connectors/test.html: LightNEasy/FCKEditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKEditor File Upload
| /editor/editor/filemanager/upload/test.html: Tadbir / File Upload
|_ /admin/jscript/upload.html: Lizard Cart/Remote File upload
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:

```
|     http://ha.ckers.org/slowloris/
|_    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open  https
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.2.16
|  Found the following possible CSRF vulnerabilities:
|
|    Path: https://192.168.2.16:443/lib/jqueryX.js?ver=3A033D
|    Form id: '+formid+'
|_   Form action:
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|  /globalSIPsettings.html: Aastra IP Phone
|  /SIPsettingsLine1.html: Aastra IP Phone
|  //system.html: CMNC-200 IP Camera
|  /siteadmin/login.html: Possible admin folder
|  /admin/index.html: Possible admin folder
|  /admin/login.html: Possible admin folder
|  /admin/admin.html: Possible admin folder
|  /admin_area/login.html: Possible admin folder
|  /admin_area/index.html: Possible admin folder
|  /admincp/index.html: Possible admin folder
|  /admin/account.html: Possible admin folder
|  /adminpanel.html: Possible admin folder
|  /webadmin.html: Possible admin folder
|  /webadmin/index.html: Possible admin folder
|  /webadmin/admin.html: Possible admin folder
|  /webadmin/login.html: Possible admin folder
|  /admin/admin_login.html: Possible admin folder
|  /admin_login.html: Possible admin folder
|  /panel-administracion/login.html: Possible admin folder
|  /admin_area/admin.html: Possible admin folder
|  /bb-admin/index.html: Possible admin folder
|  /bb-admin/login.html: Possible admin folder
|  /bb-admin/admin.html: Possible admin folder
|  /admin/home.html: Possible admin folder
|  /pages/admin/admin-login.html: Possible admin folder
|  /admin/admin-login.html: Possible admin folder
|  /admin-login.html: Possible admin folder
|  /admin/adminLogin.html: Possible admin folder
|  /adminLogin.html: Possible admin folder
|  /home.html: Possible admin folder
|  /adminarea/index.html: Possible admin folder
|  /adminarea/admin.html: Possible admin folder
|  /admin/controlpanel.html: Possible admin folder
|  /admin.html: Possible admin folder
|  /admin/cp.html: Possible admin folder
|  /cp.html: Possible admin folder
|  /moderator.html: Possible admin folder
|  /administrator/index.html: Possible admin folder
|  /administrator/login.html: Possible admin folder
|  /user.html: Possible admin folder
|  /administrator/account.html: Possible admin folder
|  /administrator.html: Possible admin folder
|  /login.html: Possible admin folder
```

| /modelsearch/login.html: Possible admin folder
| /moderator/login.html: Possible admin folder
| /adminarea/login.html: Possible admin folder
| /panel-administracion/index.html: Possible admin folder
| /panel-administracion/admin.html: Possible admin folder
| /modelsearch/index.html: Possible admin folder
| /modelsearch/admin.html: Possible admin folder
| /admincontrol/login.html: Possible admin folder
| /adm/index.html: Possible admin folder
| /adm.html: Possible admin folder
| /moderator/admin.html: Possible admin folder
| /account.html: Possible admin folder
| /controlpanel.html: Possible admin folder
| /admincontrol.html: Possible admin folder
| /test.html: Test page
| /TopToolArea.html: Alteon OS BBI (Nortell)
| /switchSystem.html: Alteon OS BBI (Nortell)
| /test/logon.html: Jetty
| /setup/password_required.html: 2WIRE GATEWAY
| /CFIDE/Administrator/startstop.html: ColdFusion Admin Console
| /HW_logo.html: Huawei HG 530
| /postinfo.html: Frontpage file or folder
| /readme.html: Interesting, a readme.
| /pligg/readme.html: Interesting, a readme.
| /digg/readme.html: Interesting, a readme.
| /news/readme.html: Interesting, a readme.
| /tinymcpuk/filemanager/browser.html: CMS Lokomedia
| /scripts/fckeditor/editor/filemanager/connectors/test.html: Digitalus CMS/FCKEditor File upload
| /scripts/fckeditor/editor/filemanager/connectors/uploadtest.html: Digitalus CMS/FCKEditor File upload
| /fckeditor/editor/filemanager/connectors/test.html: phpmotion/FCKEditor File upload
| /fckeditor/editor/filemanager/upload/test.html: Geeklog/FCKEditor File upload
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKEditor File upload
| /FCKEditor/editor/filemanager/browser/default/connectors/test.html: EgO or osCMax/FCKEditor File upload
| /_plugin/fckeditor/editor/filemanager/connectors/test.html: SweetRice/FCKEditor File upload
| /fckeditor/editor/filemanager/connectors/test.html: LightNEasy/FCKEditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKEditor File Upload
| /editor/editor/filemanager/upload/test.html: Tadbir / File Upload
|_ /admin/jscript/upload.html: Lizard Cart/Remote File upload
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:

```
|     http://ha.ckers.org/slowloris/
|_    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|           Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|           Modulus Type: Non-safe prime
|           Modulus Source: RFC5114/1024-bit DSA group with 160-bit prime order subgroup
|           Modulus Length: 1024
|           Generator Length: 1024
|           Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: LIKELY VULNERABLE
|     IDs:  OSVDB:113251  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|       TLS_FALLBACK_SCSV properly implemented
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      http://osvdb.org/113251
|_sslv2-drown:
554/tcp  open  rtsp
2020/tcp open  xinupageserver
8080/tcp open  http-proxy
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

8081/tcp open blackice-icecap
8088/tcp open radan-http
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 141.32 seconds

A.2.3 REOLINK RLC-420

Starting Nmap 7.70 (https://nmap.org) at 2019-05-01 09:34 EEST
Nmap scan report for 192.168.2.15
Host is up (0.0033s latency).
Not shown: 65527 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.6.2
443/tcp open ssl/http nginx 1.6.2
554/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
1935/tcp open rtmp?
6001/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
8000/tcp open tcpwrapped
9000/tcp open cslistener?
17823/tcp open http nginx 1.6.2
MAC Address: EC:71:DB:5F:BA:D6 (Shenzhen Baichuan Digital Technology)
Service Info: Device: webcam; CPE: cpe:/h:pelco:ide10dn

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 180.59 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-01 10:39 EEST
Nmap scan report for 192.168.2.15
Host is up (0.056s latency).
Not shown: 993 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Reolink
443/tcp open ssl/http nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=reo-link/organizationName=reo-link/stateOrProvinceName=GD/countryName=CN
| Not valid before: 2016-01-08T07:54:35
|_Not valid after: 2026-01-05T07:54:35
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_ http/1.1
| tls-nextprotoneg:
|_ http/1.1
554/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER, SET_PARAMETER
1935/tcp open rtmp?
6001/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER, SET_PARAMETER
8000/tcp open tcpwrapped
|_http-server-header: gSOAP/2.8

|_http-title: Site doesn't have a title (text/xml; charset=utf-8).
9000/tcp open cslistener?
Service Info: Device: webcam; CPE: cpe:/h:pelco:ide10dn

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 162.96 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-01 10:43 EEST
Nmap scan report for 192.168.2.15
Host is up (0.0095s latency).
Not shown: 993 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.6.2
443/tcp open ssl/http nginx 1.6.2
554/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
1935/tcp open rtmp?
6001/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
8000/tcp open tcpwrapped
9000/tcp open cslistener?
Service Info: Device: webcam; CPE: cpe:/h:pelco:ide10dn

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 5038.33 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-01 12:16 EEST
Nmap scan report for 192.168.2.15
Host is up (0.0067s latency).
Not shown: 993 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Reolink
443/tcp open ssl/http nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=reo-link/organizationName=reo-
link/stateOrProvinceName=GD/countryName=CN
| Not valid before: 2016-01-08T07:54:35
|_Not valid after: 2026-01-05T07:54:35
|_ssl-date: ERROR: Script execution failed (use -d to debug)
| tls-alpn:
|_ http/1.1
| tls-nextprotoneg:
|_ http/1.1
554/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER,
SET_PARAMETER
1935/tcp open rtmp?
6001/tcp open rtsp D-Link DCS-2130 or Pelco IDE10DN webcam rtspd
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER,
SET_PARAMETER
8000/tcp open tcpwrapped
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: gSOAP/2.8
|_http-title: Site doesn't have a title (text/xml; charset=utf-8).
9000/tcp open cslistener?

SERVICE INFO: DEVICE: WEBCAM; CPE: CPE:/H:PELCO:IDE10DN

SERVICE DETECTION PERFORMED. PLEASE REPORT ANY INCORRECT RESULTS AT HTTPS://NMAP.ORG/SUBMIT/
.
NMAP DONE: 1 IP ADDRESS (1 HOST UP) SCANNED IN 163.19 SECONDS
STARTING NMAP 7.70 (HTTPS://NMAP.ORG) AT 2019-05-03 17:13 EEST
NMAP SCAN REPORT FOR 192.168.2.15
HOST IS UP (0.00094S LATENCY).
NOT SHOWN: 993 CLOSED PORTS
PORT STATE SERVICE
80/TCP OPEN HTTP
443/TCP OPEN HTTPS
554/TCP OPEN RTSP
1935/TCP OPEN RTMP
6001/TCP OPEN X11:1
8000/TCP OPEN HTTP-ALT
9000/TCP OPEN CSLISTENER
MAC ADDRESS: EC:71:DB:5F:BA:D6 (SHENZHEN BAICHUAN DIGITAL TECHNOLOGY)
NO EXACT OS MATCHES FOR HOST (IF YOU KNOW WHAT OS IS RUNNING ON IT, SEE
HTTPS://NMAP.ORG/SUBMIT/).
TCP/IP FINGERPRINT:
OS:SCAN(V=7.70%E=4%D=5/3%OT=80%CT=1%CU=42363%PV=Y%DS=1%DC=D%G=Y%M=E
C71DB%TM
OS:=5CCC4CAC%P=X86_64-APPLE-DARWIN13.4.0)SEQ(SP=105%GCD=1%ISR=10D%TI=Z%CI=I
OS:%II=I%TS=8)OPS(O1=M5B4ST11NW3%O2=M5B4ST11NW3%O3=M5B4NNT11NW3%O4=
M5B4ST11
OS:NW3%O5=M5B4ST11NW3%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7
120%W5=71
OS:20%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW3%CC=Y%Q=)T1(R=Y
%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=
Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%
DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
R%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
)IE(R=Y
OS:%DFI=N%T=40%CD=S)

NETWORK DISTANCE: 1 HOP

OS DETECTION PERFORMED. PLEASE REPORT ANY INCORRECT RESULTS AT HTTPS://NMAP.ORG/SUBMIT/ .
NMAP DONE: 1 IP ADDRESS (1 HOST UP) SCANNED IN 14.17 SECONDS
STARTING NMAP 7.70 (HTTPS://NMAP.ORG) AT 2019-05-03 17:18 EEST
NMAP SCAN REPORT FOR 192.168.2.15
HOST IS UP (0.00097S LATENCY).
NOT SHOWN: 993 CLOSED PORTS
PORT STATE SERVICE
80/TCP OPEN HTTP
443/TCP OPEN HTTPS
554/TCP OPEN RTSP
1935/TCP OPEN RTMP
6001/TCP OPEN X11:1
8000/TCP OPEN HTTP-ALT
9000/TCP OPEN CSLISTENER

MAC Address: EC:71:DB:5F:BA:D6 (Shenzhen Baichuan Digital Technology)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=5/3%OT=80%CT=1%CU=41433%PV=Y%DS=1%DC=D%G=Y%M=E
C71DB%TM
OS:=5CCC4DCF%P=x86_64-apple-darwin13.4.0)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=I
OS:%II=I%TS=8)OPS(O1=M5B4ST11NW3%O2=M5B4ST11NW3%O3=M5B4NNT11NW3%O4=
M5B4ST11
OS:NW3%O5=M5B4ST11NW3%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7
120%W5=71
OS:20%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW3%CC=Y%Q=)T1(R=Y
%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=
Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%
DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
R%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
)IE(R=Y
OS:%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds
Starting Nmap 7.70 (https://nmap.org) at 2019-05-03 17:24 EEST
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.2.15
Host is up (0.0062s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
80/tcp open http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /main_configure.cgi: Intellinet IP Camera
| /cgi-bin/ffileman.cgi?: Ffileman Web File Manager
| /setup.cgi: Linksys Cisco Wag120n or similar
| /debug.cgi: Linksys WRT54G
| /tools_admin.cgi?: D-Link WBR-1310
| /restoreinfo.cgi: Sagem router
| /cgi-mod/view_help.cgi: Barracuda Networks Spam & Virus Firewall
| /cgi-mod/index.cgi: Barracuda Web Application Firewall
| /cgi-mod/smtp_test.cgi: Barracuda IM Firewall
| /nagios3/cgi-bin/statuswml.cgi: Nagios3
| /statmail.nsf: Lotus Domino
| /statrep.nsf: Lotus Domino
| /kbcat.cgi: ActivDesk

```
|
/includes/FCKeditor/editor/filemanager/browser/default/connectors/perl/connector.cgi:
PHPNuke/Remote File Download
|  /status/README: Interesting, a readme.
|  /statusnet/README: Interesting, a readme.
|  /state/: Potentially interesting folder
|  /stat/: Potentially interesting folder
|  /statistic/: Potentially interesting folder
|  /statistics/: Potentially interesting folder
|  /stats-bin-p/: Potentially interesting folder
|  /stats/: Potentially interesting folder
|  /stats_old/: Potentially interesting folder
|_ /status/: Potentially interesting folder
| http-fileupload-exploiter:
|
|   Couldn't find a file-type field.
|
|_  Couldn't find a file-type field.
| http-sql-injection:
|  Possible sqli for queries:
|_
http://192.168.2.15:80/js/bc_enum.js?timeVersion=00000000046%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2011-3192:
|  VULNERABLE:
|  Apache byterange filter DoS
|   State: VULNERABLE
|   IDs:  OSVDB:74721  CVE:CVE-2011-3192
|    The Apache web server is vulnerable to a denial of service attack when numerous
|    overlapping byte ranges are requested.
|   Disclosure date: 2011-08-19
|   References:
|    http://osvdb.org/74721
|    http://nessus.org/plugins/index.php?view=single&id=55976
|    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|    http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_   http://seclists.org/fulldisclosure/2011/Aug/175
443/tcp  open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| ssl-dh-params:
|  VULNERABLE:
|  Diffie-Hellman Key Exchange Insufficient Group Strength
|   State: VULNERABLE
|    Transport Layer Security (TLS) services that use Diffie-Hellman groups
|    of insufficient strength, especially those using one of a few commonly
|    shared groups, may be susceptible to passive eavesdropping attacks.
|   Check results:
|    WEAK DH GROUP 1
|        Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|        Modulus Type: Safe prime
|        Modulus Source: nginx/1024-bit MODP group with safe prime modulus
|        Modulus Length: 1024
|        Generator Length: 8
|        Public Key Length: 1024
```

```
|   References:
|_    https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: LIKELY VULNERABLE
|     IDs:  OSVDB:113251  CVE:CVE-2014-3566
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
|         for man-in-the-middle attackers to obtain cleartext data via a
|         padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|       TLS_FALLBACK_SCSV properly implemented
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       http://osvdb.org/113251
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
|_sslv2-drown:
554/tcp  open  rtsp
1935/tcp open  rtmp
6001/tcp open  X11:1
8000/tcp open  http-alt
| http-enum:
|   /blog/: Blog
|   /weblog/: Blog
|   /weblogs/: Blog
|   /wordpress/: Blog
|   /wiki/: Wiki
|   /mediawiki/: Wiki
|   /wiki/Main_Page: Wiki
|   /tikiwiki/: Tikiwiki
|   /cgi-bin/mj_wwwusr: Majordomo2 Mailing List
|   /majordomo/mj_wwwusr: Majordomo2 Mailing List
|   /j2ee/examples/servlets/: Oracle j2ee examples
|   /j2ee/examples/jsp/: Oracle j2ee examples
|   /dsc/: Trend Micro Data Loss Prevention Virtual Appliance
|   /reg_1.htm: Polycom IP phone
|   /adr.htm: Snom IP Phone
|   /line_login.htm?l=1: Snom IP Phone
|   /tbook.csv: Snom IP Phone
|   /globalSIPsettings.html: Aastra IP Phone
|   /SIPsettingsLine1.html: Aastra IP Phone
|   /websvn/: WEBSVN Repository
|   /login.stm: Belkin G Wireless Router
|   /tools_admin.php: D-Link DIR-300
|   /bsc_lan.php: D-Link DIR-300, DIR-320, DIR-615 revD
|   /Manage.tri: Linksys WRT54G2
|   //system.html: CMNC-200 IP Camera
|   /main_configure.cgi: Intellinet IP Camera
|   /OvCgi/Toolbar.exe: HP OpenView Network Node Manager
|   /frontend/x3/: cPanel
|   /awstatstotals/awstatstotals.php: AWStats Totals
|   /awstats/awstatstotals.php: AWStats Totals
```

| /AWSTATSTOTALS.PHP: AWSTATS TOTALS
| /AWSTATS/INDEX.PHP: AWSTATS TOTALS
| /AWSTATSTOTALS/INDEX.PHP: AWSTATS TOTALS
| /EGROUPWARE/: EGROUPWARE
| /CALENDAR/CAL_SEARCH.PHP: EXTCALENDAR
| /CAL_SEARCH.PHP: EXTCALENDAR
| /A_VIEWUSERS.PHP: ANDYS PHP KNOWLEDGEBASE
| /APHPKB/: ANDYS PHP KNOWLEDGEBASE
| /WEBEDITION/WE/INCLUDE/WE_MODULES/: WEB EDITION
| /WEBEDITION/: WEB EDITION
| /EXAMPLES/: POSSIBLE DOCUMENTATION FILES
| /LIGHTNEASY.PHP?DO=LOGIN: LIGHTNEASY
| /CHANNEL_DETAIL.PHP: DZTUBE
| /CGI-BIN/VCS: MITEL AUDIO AND WEB CONFERENCING (AWC)
| /OCSREPORTS/: OCS INVENTORY
| /VBSEO.PHP: VBSEO
| /FORUM/: FORUM
| /FORUMS/: FORUM
| /SMF/: FORUM
| /PHPBB/: FORUM
| /MANAGER/: POSSIBLE ADMIN FOLDER
| /ADMIN.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN/: POSSIBLE ADMIN FOLDER
| /ADMIN/ADMIN/: POSSIBLE ADMIN FOLDER
| /ADMINISTRATOR/: POSSIBLE ADMIN FOLDER
| /MODERATOR/: POSSIBLE ADMIN FOLDER
| /WEBADMIN/: POSSIBLE ADMIN FOLDER
| /ADMINAREA/: POSSIBLE ADMIN FOLDER
| /BB-ADMIN/: POSSIBLE ADMIN FOLDER
| /ADMINLOGIN/: POSSIBLE ADMIN FOLDER
| /ADMIN_AREA/: POSSIBLE ADMIN FOLDER
| /PANEL-ADMINISTRACION/: POSSIBLE ADMIN FOLDER
| /INSTADMIN/: POSSIBLE ADMIN FOLDER
| /MEMBERADMIN/: POSSIBLE ADMIN FOLDER
| /ADMINISTRATORLOGIN/: POSSIBLE ADMIN FOLDER
| /ADM/: POSSIBLE ADMIN FOLDER
| /ADMIN/ACCOUNT.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN/INDEX.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN/LOGIN.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN/ADMIN.PHP: POSSIBLE ADMIN FOLDER
| /JOOMLA/ADMINISTRATOR: POSSIBLE ADMIN FOLDER
| /LOGIN.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN_AREA/ADMIN.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN_AREA/LOGIN.PHP: POSSIBLE ADMIN FOLDER
| /SITEADMIN/LOGIN.PHP: POSSIBLE ADMIN FOLDER
| /SITEADMIN/INDEX.PHP: POSSIBLE ADMIN FOLDER
| /SITEADMIN/LOGIN.HTML: POSSIBLE ADMIN FOLDER
| /ADMIN/INDEX.HTML: POSSIBLE ADMIN FOLDER
| /ADMIN/LOGIN.HTML: POSSIBLE ADMIN FOLDER
| /ADMIN/ADMIN.HTML: POSSIBLE ADMIN FOLDER
| /ADMIN_AREA/INDEX.PHP: POSSIBLE ADMIN FOLDER
| /BB-ADMIN/INDEX.PHP: POSSIBLE ADMIN FOLDER
| /BB-ADMIN/LOGIN.PHP: POSSIBLE ADMIN FOLDER
| /BB-ADMIN/ADMIN.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN/HOME.PHP: POSSIBLE ADMIN FOLDER
| /ADMIN_AREA/LOGIN.HTML: POSSIBLE ADMIN FOLDER

| /admin_area/index.html: Possible admin folder
| /admin/controlpanel.php: Possible admin folder
| /admincp/: Possible admin folder
| /admincp/index.asp: Possible admin folder
| /admincp/index.html: Possible admin folder
| /admincp/login.php: Possible admin folder
| /admin/account.html: Possible admin folder
| /adminpanel.html: Possible admin folder
| /webadmin.html: Possible admin folder
| /webadmin/index.html: Possible admin folder
| /webadmin/admin.html: Possible admin folder
| /webadmin/login.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin_login.html: Possible admin folder
| /panel-administracion/login.html: Possible admin folder
| /admin/cp.php: Possible admin folder
| /cp.php: Possible admin folder
| /administrator/index.php: Possible admin folder
| /administrator/login.php: Possible admin folder
| /nsw/admin/login.php: Possible admin folder
| /webadmin/login.php: Possible admin folder
| /admin/admin_login.php: Possible admin folder
| /admin_login.php: Possible admin folder
| /administrator/account.php: Possible admin folder
| /administrator.php: Possible admin folder
| /admin_area/admin.html: Possible admin folder
| /pages/admin/admin-login.php: Possible admin folder
| /admin/admin-login.php: Possible admin folder
| /admin-login.php: Possible admin folder
| /bb-admin/index.html: Possible admin folder
| /bb-admin/login.html: Possible admin folder
| /bb-admin/admin.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /modelsearch/login.php: Possible admin folder
| /moderator.php: Possible admin folder
| /moderator/login.php: Possible admin folder
| /moderator/admin.php: Possible admin folder
| /account.php: Possible admin folder
| /pages/admin/admin-login.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin-login.html: Possible admin folder
| /controlpanel.php: Possible admin folder
| /admincontrol.php: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /adminLogin.html: Possible admin folder
| /home.html: Possible admin folder
| /rcjakar/admin/login.php: Possible admin folder
| /adminarea/index.html: Possible admin folder
| /adminarea/admin.html: Possible admin folder
| /webadmin.php: Possible admin folder
| /webadmin/index.php: Possible admin folder
| /webadmin/admin.php: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /cp.html: Possible admin folder

| /adminpanel.php: Possible admin folder
| /moderator.html: Possible admin folder
| /administrator/index.html: Possible admin folder
| /administrator/login.html: Possible admin folder
| /user.html: Possible admin folder
| /administrator/account.html: Possible admin folder
| /administrator.html: Possible admin folder
| /login.html: Possible admin folder
| /modelsearch/login.html: Possible admin folder
| /moderator/login.html: Possible admin folder
| /adminarea/login.html: Possible admin folder
| /panel-administracion/index.html: Possible admin folder
| /panel-administracion/admin.html: Possible admin folder
| /modelsearch/index.html: Possible admin folder
| /modelsearch/admin.html: Possible admin folder
| /admincontrol/login.html: Possible admin folder
| /adm/index.html: Possible admin folder
| /adm.html: Possible admin folder
| /moderator/admin.html: Possible admin folder
| /user.php: Possible admin folder
| /account.html: Possible admin folder
| /controlpanel.html: Possible admin folder
| /admincontrol.html: Possible admin folder
| /panel-administracion/login.php: Possible admin folder
| /wp-login.php: Possible admin folder
| /adminLogin.php: Possible admin folder
| /admin/adminLogin.php: Possible admin folder
| /adminarea/index.php: Possible admin folder
| /adminarea/admin.php: Possible admin folder
| /adminarea/login.php: Possible admin folder
| /panel-administracion/index.php: Possible admin folder
| /panel-administracion/admin.php: Possible admin folder
| /modelsearch/index.php: Possible admin folder
| /modelsearch/admin.php: Possible admin folder
| /admincontrol/login.php: Possible admin folder
| /adm/admloginuser.php: Possible admin folder
| /admloginuser.php: Possible admin folder
| /admin2.php: Possible admin folder
| /admin2/login.php: Possible admin folder
| /admin2/index.php: Possible admin folder
| /adm/index.php: Possible admin folder
| /adm.php: Possible admin folder
| /affiliate.php: Possible admin folder
| /adm_auth.php: Possible admin folder
| /memberadmin.php: Possible admin folder
| /administratorlogin.php: Possible admin folder
| /account.cfm: Possible admin folder
| /admin/account.cfm: Possible admin folder
| /admin/index.cfm: Possible admin folder
| /admin/login.cfm: Possible admin folder
| /admin/admin.cfm: Possible admin folder
| /admin.cfm: Possible admin folder
| /admin/admin_login.cfm: Possible admin folder
| /admin_login.cfm: Possible admin folder
| /adminpanel.cfm: Possible admin folder
| /admin/controlpanel.cfm: Possible admin folder

| /admincontrol.cfm: Possible admin folder
| /panel-administracion/login.cfm: Possible admin folder
| /admin/cp.cfm: Possible admin folder
| /pages/admin/admin-login.cfm: Possible admin folder
| /admincp/index.cfm: Possible admin folder
| /admincp/login.cfm: Possible admin folder
| /admin_area/admin.cfm: Possible admin folder
| /admin_area/login.cfm: Possible admin folder
| /moderator/login.cfm: Possible admin folder
| /administrator/login.cfm: Possible admin folder
| /moderator.cfm: Possible admin folder
| /modelsearch/index.cfm: Possible admin folder
| /panel-administracion/admin.cfm: Possible admin folder
| /adm/admloginuser.cfm: Possible admin folder
| /adm.cfm: Possible admin folder
| /adm_auth.cfm: Possible admin folder
| /administratorlogin.cfm: Possible admin folder
| /webadmin.cfm: Possible admin folder
| /webadmin/index.cfm: Possible admin folder
| /modelsearch/login.cfm: Possible admin folder
| /login.cfm: Possible admin folder
| /administrator.cfm: Possible admin folder
| /administrator/account.cfm: Possible admin folder
| /adminLogin.cfm: Possible admin folder
| /siteadmin/login.cfm: Possible admin folder
| /admin2/index.cfm: Possible admin folder
| /adm/index.cfm: Possible admin folder
| /admin_area/index.cfm: Possible admin folder
| /bb-admin/index.cfm: Possible admin folder
| /bb-admin/login.cfm: Possible admin folder
| /bb-admin/admin.cfm: Possible admin folder
| /siteadmin/index.cfm: Possible admin folder
| /memberadmin.cfm: Possible admin folder
| /admin2/login.cfm: Possible admin folder
| /admloginuser.cfm: Possible admin folder
| /admincontrol/login.cfm: Possible admin folder
| /administrator/index.cfm: Possible admin folder
| /modelsearch/admin.cfm: Possible admin folder
| /panel-administracion/index.cfm: Possible admin folder
| /adminarea/login.cfm: Possible admin folder
| /adminarea/admin.cfm: Possible admin folder
| /adminarea/index.cfm: Possible admin folder
| /admin/adminLogin.cfm: Possible admin folder
| /webadmin/login.cfm: Possible admin folder
| /webadmin/admin.cfm: Possible admin folder
| /user.cfm: Possible admin folder
| /controlpanel.cfm: Possible admin folder
| /moderator/admin.cfm: Possible admin folder
| /cp.cfm: Possible admin folder
| /admin-login.cfm: Possible admin folder
| /admin/admin-login.cfm: Possible admin folder
| /admin/home.cfm: Possible admin folder
| /adm1n/: Possible admin folder
| /4dm1n/: Possible admin folder
| /account.asp: Possible admin folder
| /admin/account.asp: Possible admin folder

| /admin/index.asp: Possible admin folder
| /admin/login.asp: Possible admin folder
| /admin/admin.asp: Possible admin folder
| /admin_area/admin.asp: Possible admin folder
| /admin_area/login.asp: Possible admin folder
| /admin_area/index.asp: Possible admin folder
| /bb-admin/index.asp: Possible admin folder
| /bb-admin/login.asp: Possible admin folder
| /bb-admin/admin.asp: Possible admin folder
| /admin/home.asp: Possible admin folder
| /admin/controlpanel.asp: Possible admin folder
| /admin.asp: Possible admin folder
| /pages/admin/admin-login.asp: Possible admin folder
| /admin/admin-login.asp: Possible admin folder
| /admin-login.asp: Possible admin folder
| /admin/cp.asp: Possible admin folder
| /cp.asp: Possible admin folder
| /administrator/account.asp: Possible admin folder
| /administrator.asp: Possible admin folder
| /login.asp: Possible admin folder
| /modelsearch/login.asp: Possible admin folder
| /moderator.asp: Possible admin folder
| /moderator/login.asp: Possible admin folder
| /administrator/login.asp: Possible admin folder
| /moderator/admin.asp: Possible admin folder
| /controlpanel.asp: Possible admin folder
| /user.asp: Possible admin folder
| /admincp/login.asp: Possible admin folder
| /admincontrol.asp: Possible admin folder
| /adminpanel.asp: Possible admin folder
| /webadmin.asp: Possible admin folder
| /webadmin/index.asp: Possible admin folder
| /webadmin/admin.asp: Possible admin folder
| /webadmin/login.asp: Possible admin folder
| /admin/admin_login.asp: Possible admin folder
| /admin_login.asp: Possible admin folder
| /panel-administracion/login.asp: Possible admin folder
| /adminLogin.asp: Possible admin folder
| /admin/adminLogin.asp: Possible admin folder
| /home.asp: Possible admin folder
| /adminarea/index.asp: Possible admin folder
| /adminarea/admin.asp: Possible admin folder
| /adminarea/login.asp: Possible admin folder
| /panel-administracion/index.asp: Possible admin folder
| /panel-administracion/admin.asp: Possible admin folder
| /modelsearch/index.asp: Possible admin folder
| /modelsearch/admin.asp: Possible admin folder
| /administrator/index.asp: Possible admin folder
| /admincontrol/login.asp: Possible admin folder
| /adm/admloginuser.asp: Possible admin folder
| /admloginuser.asp: Possible admin folder
| /admin2.asp: Possible admin folder
| /admin2/login.asp: Possible admin folder
| /admin2/index.asp: Possible admin folder
| /adm/index.asp: Possible admin folder
| /adm.asp: Possible admin folder

| /adm_auth.asp: Possible admin folder
| /memberadmin.asp: Possible admin folder
| /administratorlogin.asp: Possible admin folder
| /siteadmin/login.asp: Possible admin folder
| /siteadmin/index.asp: Possible admin folder
| /account.aspx: Possible admin folder
| /admin/account.aspx: Possible admin folder
| /admin/index.aspx: Possible admin folder
| /admin/login.aspx: Possible admin folder
| /admin/admin.aspx: Possible admin folder
| /admin_area/admin.aspx: Possible admin folder
| /admin_area/login.aspx: Possible admin folder
| /admin_area/index.aspx: Possible admin folder
| /bb-admin/index.aspx: Possible admin folder
| /bb-admin/login.aspx: Possible admin folder
| /bb-admin/admin.aspx: Possible admin folder
| /admin/home.aspx: Possible admin folder
| /admin/controlpanel.aspx: Possible admin folder
| /admin.aspx: Possible admin folder
| /pages/admin/admin-login.aspx: Possible admin folder
| /admin/admin-login.aspx: Possible admin folder
| /admin-login.aspx: Possible admin folder
| /admin/cp.aspx: Possible admin folder
| /cp.aspx: Possible admin folder
| /administrator/account.aspx: Possible admin folder
| /administrator.aspx: Possible admin folder
| /login.aspx: Possible admin folder
| /modelsearch/login.aspx: Possible admin folder
| /moderator.aspx: Possible admin folder
| /moderator/login.aspx: Possible admin folder
| /administrator/login.aspx: Possible admin folder
| /moderator/admin.aspx: Possible admin folder
| /controlpanel.aspx: Possible admin folder
| /user.aspx: Possible admin folder
| /admincp/index.aspx: Possible admin folder
| /admincp/login.aspx: Possible admin folder
| /admincontrol.aspx: Possible admin folder
| /adminpanel.aspx: Possible admin folder
| /webadmin.aspx: Possible admin folder
| /webadmin/index.aspx: Possible admin folder
| /webadmin/admin.aspx: Possible admin folder
| /webadmin/login.aspx: Possible admin folder
| /admin/admin_login.aspx: Possible admin folder
| /admin_login.aspx: Possible admin folder
| /panel-administracion/login.aspx: Possible admin folder
| /adminLogin.aspx: Possible admin folder
| /admin/adminLogin.aspx: Possible admin folder
| /home.aspx: Possible admin folder
| /adminarea/index.aspx: Possible admin folder
| /adminarea/admin.aspx: Possible admin folder
| /adminarea/login.aspx: Possible admin folder
| /panel-administracion/index.aspx: Possible admin folder
| /panel-administracion/admin.aspx: Possible admin folder
| /modelsearch/index.aspx: Possible admin folder
| /modelsearch/admin.aspx: Possible admin folder
| /administrator/index.aspx: Possible admin folder

| /admincontrol/login.aspx: Possible admin folder
| /adm/admloginuser.aspx: Possible admin folder
| /admloginuser.aspx: Possible admin folder
| /admin2.aspx: Possible admin folder
| /admin2/login.aspx: Possible admin folder
| /admin2/index.aspx: Possible admin folder
| /adm/index.aspx: Possible admin folder
| /adm.aspx: Possible admin folder
| /adm_auth.aspx: Possible admin folder
| /memberadmin.aspx: Possible admin folder
| /administratorlogin.aspx: Possible admin folder
| /siteadmin/login.aspx: Possible admin folder
| /siteadmin/index.aspx: Possible admin folder
| /account.jsp: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin_area/admin.jsp: Possible admin folder
| /admin_area/login.jsp: Possible admin folder
| /admin_area/index.jsp: Possible admin folder
| /bb-admin/index.jsp: Possible admin folder
| /bb-admin/login.jsp: Possible admin folder
| /bb-admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin.jsp: Possible admin folder
| /pages/admin/admin-login.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /cp.jsp: Possible admin folder
| /administrator/account.jsp: Possible admin folder
| /administrator.jsp: Possible admin folder
| /login.jsp: Possible admin folder
| /modelsearch/login.jsp: Possible admin folder
| /moderator.jsp: Possible admin folder
| /moderator/login.jsp: Possible admin folder
| /administrator/login.jsp: Possible admin folder
| /moderator/admin.jsp: Possible admin folder
| /controlpanel.jsp: Possible admin folder
| /user.jsp: Possible admin folder
| /admincp/index.jsp: Possible admin folder
| /admincp/login.jsp: Possible admin folder
| /admincontrol.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /adminpanel.jsp: Possible admin folder
| /webadmin.jsp: Possible admin folder
| /webadmin/index.jsp: Possible admin folder
| /webadmin/admin.jsp: Possible admin folder
| /webadmin/login.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin_login.jsp: Possible admin folder
| /panel-administracion/login.jsp: Possible admin folder
| /adminLogin.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /home.jsp: Possible admin folder

| /adminarea/index.jsp: Possible admin folder
| /adminarea/admin.jsp: Possible admin folder
| /adminarea/login.jsp: Possible admin folder
| /panel-administracion/index.jsp: Possible admin folder
| /panel-administracion/admin.jsp: Possible admin folder
| /modelsearch/index.jsp: Possible admin folder
| /modelsearch/admin.jsp: Possible admin folder
| /administrator/index.jsp: Possible admin folder
| /admincontrol/login.jsp: Possible admin folder
| /adm/admloginuser.jsp: Possible admin folder
| /admloginuser.jsp: Possible admin folder
| /admin2.jsp: Possible admin folder
| /admin2/login.jsp: Possible admin folder
| /admin2/index.jsp: Possible admin folder
| /adm/index.jsp: Possible admin folder
| /adm.jsp: Possible admin folder
| /adm_auth.jsp: Possible admin folder
| /memberadmin.jsp: Possible admin folder
| /administratorlogin.jsp: Possible admin folder
| /siteadmin/login.jsp: Possible admin folder
| /siteadmin/index.jsp: Possible admin folder
| /admin1.php: Possible admin folder
| /administr8.asp: Possible admin folder
| /administr8.php: Possible admin folder
| /administr8.jsp: Possible admin folder
| /administr8.aspx: Possible admin folder
| /administr8.cfm: Possible admin folder
| /administr8/: Possible admin folder
| /administer/: Possible admin folder
| /administracao.php: Possible admin folder
| /administracao.asp: Possible admin folder
| /administracao.aspx: Possible admin folder
| /administracao.cfm: Possible admin folder
| /administracao.jsp: Possible admin folder
| /administracion.php: Possible admin folder
| /administracion.asp: Possible admin folder
| /administracion.aspx: Possible admin folder
| /administracion.jsp: Possible admin folder
| /administracion.cfm: Possible admin folder
| /administrators/: Possible admin folder
| /adminpro/: Possible admin folder
| /admins/: Possible admin folder
| /admins.cfm: Possible admin folder
| /admins.php: Possible admin folder
| /admins.jsp: Possible admin folder
| /admins.asp: Possible admin folder
| /admins.aspx: Possible admin folder
| /maintenance/: Possible admin folder
| /Lotus_Domino_Admin/: Possible admin folder
| /hpwebjetadmin/: Possible admin folder
| /_admin/: Possible admin folder
| /_administrator/: Possible admin folder
| /_administrador/: Possible admin folder
| /_admins/: Possible admin folder
| /_administrators/: Possible admin folder
| /_administradores/: Possible admin folder

| /_ADMINISTRACION/: POSSIBLE ADMIN FOLDER
| /_4DM1N/: POSSIBLE ADMIN FOLDER
| /_ADM1N/: POSSIBLE ADMIN FOLDER
| /_ADMIN/: POSSIBLE ADMIN FOLDER
| /SYSTEM_ADMINISTRATION/: POSSIBLE ADMIN FOLDER
| /SYSTEM-ADMINISTRATION/: POSSIBLE ADMIN FOLDER
| /SYSTEM-ADMIN/: POSSIBLE ADMIN FOLDER
| /SYSTEM-ADMINS/: POSSIBLE ADMIN FOLDER
| /SYSTEM-ADMINISTRATORS/: POSSIBLE ADMIN FOLDER
| /ADMINISTRACION-SISTEMA/: POSSIBLE ADMIN FOLDER
| /ADMINISTRACION/: POSSIBLE ADMIN FOLDER
| /ADMIN/: POSSIBLE ADMIN FOLDER
| /ADMINISTRATOR/: POSSIBLE ADMIN FOLDER
| /MANAGER/: POSSIBLE ADMIN FOLDER
| /ADM/: POSSIBLE ADMIN FOLDER
| /SYSTEMADMIN/: POSSIBLE ADMIN FOLDER
| /ADMINLOGIN.ASP: POSSIBLE ADMIN FOLDER
| /ADMINLOGIN.PHP: POSSIBLE ADMIN FOLDER
| /ADMINLOGIN.JSP: POSSIBLE ADMIN FOLDER
| /ADMINLOGIN.ASPX: POSSIBLE ADMIN FOLDER
| /ADMINLOGIN.CFM: POSSIBLE ADMIN FOLDER
| /ADMIN108/: POSSIBLE ADMIN FOLDER
| /PEC_ADMIN/: POSSIBLE ADMIN FOLDER
| /SYSTEM/ADMIN/: POSSIBLE ADMIN FOLDER
| /PLOG-ADMIN/: POSSIBLE ADMIN FOLDER
| /ESADMIN/: POSSIBLE ADMIN FOLDER
| /AXIS2-ADMIN/: POSSIBLE ADMIN FOLDER
| /_SYS/: POSSIBLE ADMIN FOLDER
| /ADMIN_CP.ASP: POSSIBLE ADMIN FOLDER
| /SITECORE/ADMIN/: POSSIBLE ADMIN FOLDER
| /SITECORE/LOGIN/ADMIN/: POSSIBLE ADMIN FOLDER
| /B.SQL: POSSIBLE DATABASE BACKUP
| /DB.SQL: POSSIBLE DATABASE BACKUP
| /DDB.SQL: POSSIBLE DATABASE BACKUP
| /USERS.SQL: POSSIBLE DATABASE BACKUP
| /DATABASE.SQL: POSSIBLE DATABASE BACKUP
| /MYSQL.SQL: POSSIBLE DATABASE BACKUP
| /DUMP.SQL: POSSIBLE DATABASE BACKUP
| /RESPALDO.SQL: POSSIBLE DATABASE BACKUP
| /DATA.SQL: POSSIBLE DATABASE BACKUP
| /OLD.SQL: POSSIBLE DATABASE BACKUP
| /USUARIOS.SQL: POSSIBLE DATABASE BACKUP
| /BDB.SQL: POSSIBLE DATABASE BACKUP
| /1.SQL: POSSIBLE DATABASE BACKUP
| /ADMIN/DOWNLOAD/BACKUP.SQL: POSSIBLE DATABASE BACKUP
| /CLIENTACCESSPOLICY.XML: MICROSOFT SILVERLIGHT CROSSDOMAIN POLICY
| /ATOM/: RSS OR ATOM FEED
| /ATOM.ASPX: RSS OR ATOM FEED
| /ATOM.PHP: RSS OR ATOM FEED
| /ATOM.XML: RSS OR ATOM FEED
| /ATOM.JSP: RSS OR ATOM FEED
| /RSS/: RSS OR ATOM FEED
| /RSS.ASPX: RSS OR ATOM FEED
| /RSS.PHP: RSS OR ATOM FEED
| /RSS.XML: RSS OR ATOM FEED
| /RSS.JSP: RSS OR ATOM FEED

| /LOGIN/: LOGIN PAGE
| /LOGIN.HTM: LOGIN PAGE
| /LOGIN.JSP: LOGIN PAGE
| /TEST.ASP: TEST PAGE
| /TEST.CLASS: TEST PAGE
| /TEST/: TEST PAGE
| /TEST.HTM: TEST PAGE
| /TEST.HTML: TEST PAGE
| /TEST.PHP: TEST PAGE
| /TEST.TXT: TEST PAGE
| /WEBMAIL/: MAIL FOLDER
| /MAIL/: MAIL FOLDER
| /LOG/: LOGS
| /LOG.HTM: LOGS
| /LOG.PHP: LOGS
| /LOG.ASP: LOGS
| /LOG.ASPX: LOGS
| /LOG.JSP: LOGS
| /LOGS/: LOGS
| /LOGS.HTM: LOGS
| /LOGS.PHP: LOGS
| /LOGS.ASP: LOGS
| /LOGS.ASPX: LOGS
| /LOGS.JSP: LOGS
| /WWWLOG/: LOGS
| /WWWLOGS/: LOGS
| /MAIL_LOG_FILES/: LOGS
| /IMAGES/RAILS.PNG: RUBY ON RAILS
| /MONO/: MONO
| /ROBOTS.TXT: ROBOTS FILE
| /CROSSDOMAIN.XML: ADOBE FLASH CROSSDOMAIN POLICY
| /CSS/CAKE.GENERIC.CSS: CAKEPHP APPLICATION
| /IMG/CAKE.ICON.GIF: CAKEPHP APPLICATION
| /IMG/CAKE.ICON.PNG: CAKEPHP APPLICATION
| /JS/VENDORS.PHP: CAKEPHP APPLICATION
| /CGI-BIN/FFILEMAN.CGI?: FFILEMAN WEB FILE MANAGER
| /FSHOW.PHP: HORIZON WEB APP
| /ADMIN/UPLOAD.PHP: ADMIN FILE UPLOAD
| /UPLOAD_MULTIPLE_JS.PHP: NAS UPLOADER
| /UPLOADTESTER.ASP: FREE ASP UPLOAD SHELL
| /INFO.PHP: POSSIBLE INFORMATION FILE
| /PHPINFO.PHP: POSSIBLE INFORMATION FILE
| /KUSABAX/MANAGE_PAGE.PHP: KUSABAX IMAGE BOARD
| /PLUS/LURKING.PHP: PHPMYCHAT PLUS
| /ADM/BARRA/ASSETMANAGER/ASSETMANAGER.PHP: 360 WEB MANAGER
| /EYEOS/: POSSIBLE EYEOS INSTALLATION
| /NETWARE.HTM: PLANET FPS-1101
| /SETUP.CGI: LINKSYS CISCO WAG120N OR SIMILAR
| /DEBUG.CGI: LINKSYS WRT54G
| /EHCP/?OP=APPLYFORFTPACCOUNT: EASY HOSTING CONTROL PANEL
| /EHCP/?OP=APPLYFORACCOUNT: EASY HOSTING CONTROL PANEL
| /EHCP/?OP=APPLYFORDOMAINACCOUNT: EASY HOSTING CONTROL PANEL
| /VHOSTS/EHCP/?OP=APPLYFORFTPACCOUNT: EASY HOSTING CONTROL PANEL
| /VHOSTS/EHCP/?OP=APPLYFORACCOUNT: EASY HOSTING CONTROL PANEL
| /VHOSTS/EHCP/?OP=APPLYFORDOMAINACCOUNT: EASY HOSTING CONTROL PANEL
| /TOOLS_ADMIN.CGI?: D-LINK WBR-1310

| /appServer/jvmReport.jsf?instanceName=server&pageTitle=JVM%20Report: Oracle GlashFish Server Information
| /common/appServer/jvmReport.jsf?pageTitle=JVM%20Report: Oracle GlashFish Server Information
| /common/appServer/jvmReport.jsf?reportType=summary&instanceName=server: Oracle GlashFish Server Information
| /console/login/loginForm.jsp: Oracle WebLogic Server Administration Console
| /browserId/wizardForm.jhtml: Cisco Collaboration Server
| /webline/html/forms/callback.jhtml: Cisco Collaboration Server
| /webline/html/forms/callbackICM.jhtml: Cisco Collaboration Server
| /webline/html/agent/AgentFrame.jhtml: Cisco Collaboration Server
| /webline/html/agent/default/badlogin.jhtml: Cisco Collaboration Server
| /callme/callForm.jhtml: Cisco Collaboration Server
| /webline/html/multichatui/nowDefunctWindow.jhtml: Cisco Collaboration Server
| /browserId/wizard.jhtml: Cisco Collaboration Server
| /admin/CiscoAdmin.jhtml: Cisco Collaboration Server
| /msccallme/mscCallForm.jhtml: Cisco Collaboration Server
| /webline/html/admin/wcs/LoginPage.jhtml: Cisco Collaboration Server
| /restoreinfo.cgi: Sagem router
| /confirminvite.php: phpMyBitTorrent
| /sourcebans/: SourceBans - Steam server application
| /swfupload/index.php: SWFUpload
| /mymarket/shopping/index.php: MyMarket
| /myshop_start.php: FozzCom shopping
| /piranha/secure/passwd.php3: RedHat Piranha Virtual Server
| /cgi-bin/ck/mimencode: ContentKeeper Web Appliance
| /cgi-bin/masterCGI?: Alcatel-Lucent OmniPCX Enterprise
| /tiny_mce/plugins/filemanager/: Tiny MCE File Upload
| /upload/scp/ajax.php: osTicket / AJAX File Upload
| /cgi-mod/view_help.cgi: Barracuda Networks Spam & Virus Firewall
| /cgi-mod/index.cgi: Barracuda Web Application Firewall
| /cgi-mod/smtp_test.cgi: Barracuda IM Firewall
| /TopToolArea.html: Alteon OS BBI (Nortell)
| /switchSystem.html: Alteon OS BBI (Nortell)
| /intruvert/jsp/module/Login.jsp: McAfee Network Security Manager
| /ajaxfilemanager/: AJAX File Manager
| /upload/data/settings.cdb: CF Image Hosting DB
| /fm.php: Simple File Manager
| /nagios3/cgi-bin/statuswml.cgi: Nagios3
| /nagios3/: Nagios3
| /test/logon.html: Jetty
| /cal_cat.php: Calendarix
| /calendar/cal_cat.php: Calendarix
| /cal/cal_cat.php: Calendarix
| /private/sdc.tgz: IBM Bladecenter Management Logs
| /cacti/: Cacti Web Monitoring
| /cgi-bin/awstats.pl: AWStats
| /wiki/rankings.php: Bit Weaver
| /reqdetails.php: BtiTracker
| /shared/help.php: OpenBiblio/WebBiblio Subject Gateway System
| /seti.php: PHP SETI@home
| /imc/: 3Com Intelligent Management Center
| /imcws/: 3Com Intelligent Management Center
| /partymgr/: Apache OFBiz
| /Base/upload.php: MassMirror Uploader
| /Base/example_1.php: MassMirror Uploader

| /YUI-UPLOAD/HTML: YUI IMAGES / FILE UPLOAD
| /TOOLS/FILEMANAGER/SKINS/MOBILE/ADMIN1.TEMPLATE.PHP: ISPCP OMEGA
| /UPLOADIFY/: UPLOADIFY
| /SYSSITE/: SHOPEX
| /UPDOWN.PHP: PHP UPLOADER DOWNLOADER
| /MODULES/DOCMANAGER/DOCTYPETEMPLATES/MYUPLOADEDFILE: ACHIEVO
| /REQWEBHELP/ADVANCED/WORKINGSET.JSP: IBM RATIONAL REQUISITEPRO/REQWEBHELP
| /DHOST/: NOVELL EDIRECTORY
| /ENGINE/API/API.CLASS.PHP: DATALIFEENGINE
| /JSFT_RESOURCE.JSF: JSFTEMPLATING/MOJARRA SCALES/GLASSFISH APPLICATION SERVER
| /SCALES_STATIC_RESOURCE.JSF: JSFTEMPLATING/MOJARRA SCALES/GLASSFISH APPLICATION SERVER
| /SETUP/PASSWORD_REQUIRED.HTML: 2WIRE GATEWAY
| /ZP-CORE/: ZEN PHOTO
| /AMEMBER/: AMEMBER
| /.HGIGNORE: REVISION CONTROL IGNORE FILE
| /.GITIGNORE: REVISION CONTROL IGNORE FILE
| /.BZRIGNORE: REVISION CONTROL IGNORE FILE
| /ARCSIGHT/: ARCSIGHT
| /ARCSIGHT/IMAGES/LOGO-LOGIN-ARCSIGHT.GIF: ARCSIGHT
| /ARCSIGHT/IMAGES/NAVBAR-ICON-LOGOUT-ON.GIF: ARCSIGHT
| /IMAGES/LOGO-ARCSIGHT.GIF: ARCSIGHT
| /LOGGER/MONITOR.FTL: ARCSIGHT
| /BEEF/: BEEF BROWSER EXPLOITATION FRAMEWORK
| /BEEF/: BEEF BROWSER EXPLOITATION FRAMEWORK
| /BEEF/IMAGES/BEEF.GIF: BEEF BROWSER EXPLOITATION FRAMEWORK
| /GFX/FORM_TOP_LEFT_CORNER.GIF: SECUNIA NSI
| /GFX/LOGOUT_24.PNG: SECUNIA NSI
| /GFX/NEW_LOGO.GIF: SECUNIA NSI
| /JAVASCRIPT/SORTTABLE.JS: SECUNIA NSI
| /IMAGES/BTN_HELP_NML.GIF: IBM PROVENTIA
| /IMAGES/HDR_ICON_HOMEG.GIF: IBM PROVENTIA
| /SPCONTROL.PHP: IBM PROVENTIA
| /IMAGES/ISSLOGO.GIF: IBM PROVENTIA
| /DEPLOYMENTMANAGER/: IBM PROVENTIA
| /I18N/EN/CSS/FOUNDSTONE.CSS: FOUNDSTONE
| /I18N/EN/IMAGES/EXTERNAL_NAV_SQUARE.GIF: FOUNDSTONE
| /OFFICESCAN/CONSOLE/HTML/CGI/CGICHKMASTERPWD.EXE: TREND MICRO OFFICESCAN SERVER
| /OFFICESCAN/CONSOLE/HTML/CLIENTINSTALL/OFFICESCANNT.HTM: TREND MICRO OFFICESCAN SERVER
| /OFFICESCAN/CONSOLE/HTML/IMAGES/ICON_REFRESH.GIF: TREND MICRO OFFICESCAN SERVER
| /PICTS/BC_BWLOGOREV.GIF: BLUECOAT REPORTER
| /PICTS/MENU_LEAF.GIF: BLUECOAT REPORTER
| /THEME/IMAGES/EN/LOGIN1.GIF: FORTINET VPN/FIREWALL
| /NESSUSCLIENT.SWF: NESSUS
| /DOTDEFENDER/: DOTDEFENDER WEB APPLICATION FIREWALL
| /VMWARE/: VMWARE
| /VMWARE/IMX/VMWARE_BOXES-16X16.PNG: VMWARE
| /UI/: VMWARE
| /UI/IMX/VMWARELOGO-16X16.PNG: VMWARE
| /UI/IMX/VMWAREPAPERBAGLOGO-16X16.PNG: VMWARE
| /UI/VMANAGE.DO: VMWARE
| /CLIENT/VMWARE-VICLIENT.EXE: VMWARE
| /EN/WELCOMERES.JS: VMWARE
| /CITRIX/: CITRIX
| /CITRIX/: CITRIX
| /CITRIX/METAFRAME/AUTH/LOGIN.ASPX: CITRIX
| /IMAGES/CTXHEADER01.JPG: CITRIX

| /images/Safeword_Token.jpg: Citrix
| /sw/auth/login.aspx: Citrix
| /vpn/images/AccessGateway.ico: Citrix
| /citrix/AccessPlatform/auth/clientscripts/: Citrix
| /AccessPlatform/auth/clientscripts/: Citrix
| /Citrix//AccessPlatform/auth/clientscripts/cookies.js: Citrix
| /Citrix/AccessPlatform/auth/clientscripts/login.js: Citrix
| /Citrix/PNAgent/config.xml: Citrix
| /cgi-bin/image/shikaku2.png: TeraStation PRO RAID 0/1/5 Network Attached Storage
| /config/public/usergrp.gif: AXIS StorPoint
| /pictures/buttons/file_view_mark.gif: AXIS StorPoint
| /cpqlogin.htm?RedirectUrl=/&RedirectQueryString=: HP System Management Homepage
| /hplogo.gif: HP System Management Homepage
| /ie_index.htm: HP Integrated Lights Out
| /ilo.gif: HP Integrated Lights Out
| /images/icon_server_connected.gif: HP Blade Enclosure
| /mxhtml/images/signin_logo.gif: HP Insight Manager
| /mxhtml/images/status_critical_15.gif: HP Insight Manager
| /mxportal/home/en_US/servicetools.gif: HP Insight Manager
| /mxportal/home/MxPortalFrames.jsp: HP Insight Manager
| /xymon/menu/menu.css: Xymon
| /rrc.htm: Raritan Remote Client
| /manager/html/upload: Apache Tomcat
| /manager/html: Apache Tomcat
| /axis2/axis2-web/HappyAxis.jsp: Apache Axis2
| /axis2/: Apache Axis2
| /happyaxis.jsp: Apache Axis2
| /web-console/ServerInfo.jsp: JBoss Console
| /web-console/Invoker: JBoss Console
| /invoker/JMXInvokerServlet: JBoss Console
| /invoker/: JBoss Console
| /jmx-console/: JBoss Console
| /admin-console/: JBoss Console
| /CFIDE/administrator/enter.cfm: ColdFusion Admin Console
| /CFIDE/administrator/entman/index.cfm: ColdFusion Admin Console
| /cfide/install.cfm: ColdFusion Admin Console
| /CFIDE/administrator/archives/index.cfm: ColdFusion Admin Console
| /CFIDE/wizards/common/_logintowizard.cfm: ColdFusion Admin Console
| /CFIDE/componentutils/login.cfm: ColdFusion Admin Console
| /CFIDE/Administrator/startstop.html: ColdFusion Admin Console
| /flexfm/: Flex File Manager
| /lib/usermanagement/userInfo.php: Testlink TestManagement
| /security/xamppsecurity.php: XAMPP
| /dm-albums/dm-albums.php: DM FileManager
| /x_logo.gif: Xerox printer
| /gif/hp.gif: HP Printer
| /gif/hp_invent_logo.gif: HP Printer
| /gif/printer.gif: HP Printer
| /hp/device/this.LCDispatcher: HP Printer
| /hp/device/webAccess/index.htm: HP Printer
| /PageSelector.class: HP Printer
| /images/lexbold.gif: Lexmark Printer
| /images/lexlogo.gif: Lexmark Printer
| /images/printer.gif: Lexmark Printer
| /printer/image: Lexmark Printer
| /images/mute_alloff.gif: NEC Projector

| /images/pic_bri.gif: NEC Projector
| /scanweb/images/scanwebtm.gif: SCAN Web (Webcam)
| /view/index.shtml: Axis 212 PTZ Network Camera
| /phpmyadmin/: phpMyAdmin
| /phpMyAdmin/: phpMyAdmin
| /PHPMyAdmin/: phpMyAdmin
| /PMA/: phpMyAdmin
| /pma/: phpMyAdmin
| /dbadmin/: phpMyAdmin
| /myadmin/: phpMyAdmin
| /php-my-admin/: phpMyAdmin
| /phpMyAdmin2/: phpMyAdmin
| /phpMyAdmin-2/: phpMyAdmin
| /phpMyAdmin-2.2.3/: phpMyAdmin
| /phpMyAdmin-2.2.6/: phpMyAdmin
| /phpMyAdmin-2.5.1/: phpMyAdmin
| /phpMyAdmin-2.5.4/: phpMyAdmin
| /phpMyAdmin-2.5.5-rc1/: phpMyAdmin
| /phpMyAdmin-2.5.5-rc2/: phpMyAdmin
| /phpMyAdmin-2.5.5/: phpMyAdmin
| /phpMyAdmin-2.5.5-pl1/: phpMyAdmin
| /phpMyAdmin-2.5.6-rc1/: phpMyAdmin
| /phpMyAdmin-2.5.6-rc2/: phpMyAdmin
| /phpMyAdmin-2.5.6/: phpMyAdmin
| /phpMyAdmin-2.5.7/: phpMyAdmin
| /phpMyAdmin-2.5.7-pl1/: phpMyAdmin
| /phpMyAdmin-2.6.0-alpha/: phpMyAdmin
| /phpMyAdmin-2.6.0-alpha2/: phpMyAdmin
| /phpMyAdmin-2.6.0-beta1/: phpMyAdmin
| /phpMyAdmin-2.6.0-beta2/: phpMyAdmin
| /phpMyAdmin-2.6.0-rc1/: phpMyAdmin
| /phpMyAdmin-2.6.0-rc2/: phpMyAdmin
| /phpMyAdmin-2.6.0-rc3/: phpMyAdmin
| /phpMyAdmin-2.6.0/: phpMyAdmin
| /phpMyAdmin-2.6.0-pl1/: phpMyAdmin
| /phpMyAdmin-2.6.0-pl2/: phpMyAdmin
| /phpMyAdmin-2.6.0-pl3/: phpMyAdmin
| /phpMyAdmin-2.6.1-rc1/: phpMyAdmin
| /phpMyAdmin-2.6.1-rc2/: phpMyAdmin
| /phpMyAdmin-2.6.1/: phpMyAdmin
| /phpMyAdmin-2.6.1-pl1/: phpMyAdmin
| /phpMyAdmin-2.6.1-pl2/: phpMyAdmin
| /phpMyAdmin-2.6.1-pl3/: phpMyAdmin
| /phpMyAdmin-2.6.2-rc1/: phpMyAdmin
| /phpMyAdmin-2.6.2-beta1/: phpMyAdmin
| /phpMyAdmin-2.6.2/: phpMyAdmin
| /phpMyAdmin-2.6.2-pl1/: phpMyAdmin
| /phpMyAdmin-2.6.3/: phpMyAdmin
| /phpMyAdmin-2.6.3-rc1/: phpMyAdmin
| /phpMyAdmin-2.6.3-pl1/: phpMyAdmin
| /phpMyAdmin-2.6.4-rc1/: phpMyAdmin
| /phpMyAdmin-2.6.4-pl1/: phpMyAdmin
| /phpMyAdmin-2.6.4-pl2/: phpMyAdmin
| /phpMyAdmin-2.6.4-pl3/: phpMyAdmin
| /phpMyAdmin-2.6.4-pl4/: phpMyAdmin
| /phpMyAdmin-2.6.4/: phpMyAdmin

| /phpMyAdmin-2.7.0-beta1/: phpMyAdmin
| /phpMyAdmin-2.7.0-rc1/: phpMyAdmin
| /phpMyAdmin-2.7.0-pl1/: phpMyAdmin
| /phpMyAdmin-2.7.0-pl2/: phpMyAdmin
| /phpMyAdmin-2.7.0/: phpMyAdmin
| /phpMyAdmin-2.8.0-beta1/: phpMyAdmin
| /phpMyAdmin-2.8.0-rc1/: phpMyAdmin
| /phpMyAdmin-2.8.0-rc2/: phpMyAdmin
| /phpMyAdmin-2.8.0/: phpMyAdmin
| /phpMyAdmin-2.8.0.1/: phpMyAdmin
| /phpMyAdmin-2.8.0.2/: phpMyAdmin
| /phpMyAdmin-2.8.0.3/: phpMyAdmin
| /phpMyAdmin-2.8.0.4/: phpMyAdmin
| /phpMyAdmin-2.8.1-rc1/: phpMyAdmin
| /phpMyAdmin-2.8.1/: phpMyAdmin
| /phpMyAdmin-2.8.2/: phpMyAdmin
| /sqlmanager/: phpMyAdmin
| /php-myadmin/: phpMyAdmin
| /phpmy-admin/: phpMyAdmin
| /mysqladmin/: phpMyAdmin
| /mysql-admin/: phpMyAdmin
| /websql/: phpMyAdmin
| /_phpmyadmin/: phpMyAdmin
| /footer1.gif: (possible) Oracle Web server
| /homepage.nsf/homePage.gif?OpenImageResource: Lotus Domino
| /icons/ecblank.gif: Lotus Domino
| /852566C90012664F: Lotus Domino
| /admin4.nsf: Lotus Domino
| /admin5.nsf: Lotus Domino
| /admin.nsf: Lotus Domino
| /agentrunner.nsf: Lotus Domino
| /alog.nsf: Lotus Domino
| /a_domlog.nsf: Lotus Domino
| /bookmark.nsf: Lotus Domino
| /busytime.nsf: Lotus Domino
| /catalog.nsf: Lotus Domino
| /certa.nsf: Lotus Domino
| /certlog.nsf: Lotus Domino
| /certsrv.nsf: Lotus Domino
| /chatlog.nsf: Lotus Domino
| /clbusy.nsf: Lotus Domino
| /cldbdir.nsf: Lotus Domino
| /clusta4.nsf: Lotus Domino
| /collect4.nsf: Lotus Domino
| /da.nsf: Lotus Domino
| /dba4.nsf: Lotus Domino
| /dclf.nsf: Lotus Domino
| /DEASAppDesign.nsf: Lotus Domino
| /DEASLog01.nsf: Lotus Domino
| /DEASLog02.nsf: Lotus Domino
| /DEASLog03.nsf: Lotus Domino
| /DEASLog04.nsf: Lotus Domino
| /DEASLog05.nsf: Lotus Domino
| /DEASLog.nsf: Lotus Domino
| /decsadm.nsf: Lotus Domino
| /decslog.nsf: Lotus Domino

| /DEESAdmin.nsf: Lotus Domino
| /dirassist.nsf: Lotus Domino
| /doladmin.nsf: Lotus Domino
| /domadmin.nsf: Lotus Domino
| /domcfg.nsf: Lotus Domino
| /domguide.nsf: Lotus Domino
| /domlog.nsf: Lotus Domino
| /dspug.nsf: Lotus Domino
| /events4.nsf: Lotus Domino
| /events5.nsf: Lotus Domino
| /events.nsf: Lotus Domino
| /event.nsf: Lotus Domino
| /homepage.nsf: Lotus Domino
| /iNotes/Forms5.nsf/$DefaultNav: Lotus Domino
| /jotter.nsf: Lotus Domino
| /leiadm.nsf: Lotus Domino
| /leilog.nsf: Lotus Domino
| /leivlt.nsf: Lotus Domino
| /log4a.nsf: Lotus Domino
| /log.nsf: Lotus Domino
| /l_domlog.nsf: Lotus Domino
| /mab.nsf: Lotus Domino
| /mail10.box: Lotus Domino
| /mail1.box: Lotus Domino
| /mail2.box: Lotus Domino
| /mail3.box: Lotus Domino
| /mail4.box: Lotus Domino
| /mail5.box: Lotus Domino
| /mail6.box: Lotus Domino
| /mail7.box: Lotus Domino
| /mail8.box: Lotus Domino
| /mail9.box: Lotus Domino
| /mail.box: Lotus Domino
| /msdwda.nsf: Lotus Domino
| /mtatbls.nsf: Lotus Domino
| /mtstore.nsf: Lotus Domino
| /names.nsf: Lotus Domino
| /nntppost.nsf: Lotus Domino
| /nntp/nd000001.nsf: Lotus Domino
| /nntp/nd000002.nsf: Lotus Domino
| /nntp/nd000003.nsf: Lotus Domino
| /ntsync45.nsf: Lotus Domino
| /perweb.nsf: Lotus Domino
| /qpadmin.nsf: Lotus Domino
| /quickplace/quickplace/main.nsf: Lotus Domino
| /reports.nsf: Lotus Domino
| /sample/siregw46.nsf: Lotus Domino
| /schema50.nsf: Lotus Domino
| /setupweb.nsf: Lotus Domino
| /setup.nsf: Lotus Domino
| /smbcfg.nsf: Lotus Domino
| /smconf.nsf: Lotus Domino
| /smency.nsf: Lotus Domino
| /smhelp.nsf: Lotus Domino
| /smmsg.nsf: Lotus Domino
| /smquar.nsf: Lotus Domino

| /SMSOLAR.NSF: LOTUS DOMINO
| /SMTIME.NSF: LOTUS DOMINO
| /SMTPIBWQ.NSF: LOTUS DOMINO
| /SMTPOBWQ.NSF: LOTUS DOMINO
| /SMTP.BOX: LOTUS DOMINO
| /SMTP.NSF: LOTUS DOMINO
| /SMVLOG.NSF: LOTUS DOMINO
| /SRVNAM.HTM: LOTUS DOMINO
| /STATMAIL.NSF: LOTUS DOMINO
| /STATREP.NSF: LOTUS DOMINO
| /STAUTHS.NSF: LOTUS DOMINO
| /STAUTHT.NSF: LOTUS DOMINO
| /STCONFIG.NSF: LOTUS DOMINO
| /STCONF.NSF: LOTUS DOMINO
| /STDNASET.NSF: LOTUS DOMINO
| /STDOMINO.NSF: LOTUS DOMINO
| /STLOG.NSF: LOTUS DOMINO
| /STREG.NSF: LOTUS DOMINO
| /STSRC.NSF: LOTUS DOMINO
| /USERREG.NSF: LOTUS DOMINO
| /VPUSERINFO.NSF: LOTUS DOMINO
| /WEBADMIN.NSF: LOTUS DOMINO
| /WEB.NSF: LOTUS DOMINO
| /.NSF/../WINNT/WIN.INI: LOTUS DOMINO
| /ICONS/ECBLANK.GIF: LOTUS DOMINO
| /_LAYOUTS/IMAGES/HELPICON.GIF: MS SHAREPOINT
| /PAGES/DEFAULT.ASPX: MS SHAREPOINT
| /PUBLISHINGIMAGES/NEWSARTICLEIMAGE.JPG: MS SHAREPOINT
| /_ADMIN/OPERATIONS.ASPX: MS SHAREPOINT
| /_APP_BIN: MS SHAREPOINT
| /_CONTROLTEMPLATES: MS SHAREPOINT
| /_LAYOUTS: MS SHAREPOINT
| /_LAYOUTS/VIEWLSTS.ASPX: MS SHAREPOINT
| /FORMS/ALLITEMS.ASPX: MS SHAREPOINT
| /FORMS/WEBFLDR.ASPX: MS SHAREPOINT
| /FORMS/MOD-VIEW.ASPX: MS SHAREPOINT
| /FORMS/MY-SUB.ASPX: MS SHAREPOINT
| /PAGES/CATEGORYRESULTS.ASPX: MS SHAREPOINT
| /CATEGORIES/VIEWCATEGORY.ASPX: MS SHAREPOINT
| /SITEDIRECTORY: MS SHAREPOINT
| /EDITDOCS.ASPX: MS SHAREPOINT
| /WORKFLOWTASKS/ALLITEMS.ASPX: MS SHAREPOINT
| /LISTS/TASKS/: MS SHAREPOINT
| /CATEGORIES/ALLCATEGORIES.ASPX: MS SHAREPOINT
| /CATEGORIES/SOMEOTHERDIR/ALLCATEGORIES.ASPX: MS SHAREPOINT
| /MYCATEGORIES.ASPX: MS SHAREPOINT
| /LISTS/: MS SHAREPOINT
| /LISTS/ALLITEMS.ASPX: MS SHAREPOINT
| /LISTS/DEFAULT.ASPX: MS SHAREPOINT
| /LISTS/ALLPOSTS.ASPX: MS SHAREPOINT
| /LISTS/ARCHIVE.ASPX: MS SHAREPOINT
| /LISTS/BYAUTHOR.ASPX: MS SHAREPOINT
| /LISTS/CALENDAR.ASPX: MS SHAREPOINT
| /LISTS/MOD-VIEW.ASPX: MS SHAREPOINT
| /LISTS/MYPOSTS.ASPX: MS SHAREPOINT
| /LISTS/MY-SUB.ASPX: MS SHAREPOINT

| /lists/allcomments.aspx: MS Sharepoint
| /lists/mycomments.aspx: MS Sharepoint
| /_layouts/userdisp.aspx: MS Sharepoint
| /_layouts/help.aspx: MS Sharepoint
| /_layouts/download.aspx: MS Sharepoint
| /projectserver/Home/HomePage.asp: MS Project Server
| /projectserver/images/branding.gif: MS Project Server
| /projectserver/images/pgHome.gif: MS Project Server
| /projectserver/images/pgTask.gif: MS Project Server
| /projectserver/Tasks/Taskspage.asp: MS Project Server
| /exchweb/bin/auth/owalogon.asp: Outlook Web Access
| /images/outlook.jpg: Outlook Web Access
| /owa/8.1.375.2/themes/base/lgntopl.gif: Outlook Web Access
| /owa/: Outlook Web Access
| /tsweb/: Remote Desktop Web Connection
| /reportserver/: Microsoft SQL Report Service
| /HW_logo.html: Huawei HG 530
| /icons/icon_set_up_2701XX_01.gif: 2WIRE 2701HG
| /icons/icon_homeportal_2701XX.gif: 2WIRE 2701HG
| /es/images/nav_sl_home_network_01.gif: 2WIRE 2701HG
| /en/images/nav_sl_home_network_01.gif: 2WIRE 2701HG
| /images/stxx__xl.gif: Thomson TG585
| /images/bbc__xl.gif: Thomson TG585
|
..%2f..%2f..%2f..%2f..%2f..%2f..%2f/var/mobile/Library/AddressBook/AddressBook.sqlitedb: Possible iPhone/iPod/iPad generic file sharing app Directory Traversal (iOS)
| /cmspages.php: 2Point Solutions CMS
| /sc_webcat/ecat/cms_view.php: Webcat
| /kbcat.cgi: ActivDesk
| /forum_answer.php?que_id=1: Guru JustAnswer
| /templates1/view_product.php: HB ECommerce
| /escort-profile.php: First Escort Marketing CMS
| /pages/indexheader.php: Green Pants CMS
| /pages/searcher.php: Green Pants CMS
| /pages/indexviewentry.php: Green Pants CMS
| /tinymcpuk/filemanager/browser.html: CMS Lokomedia
| /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
| /leftmenubody.php: Quicktech
| /dsp_page.cfm: Alcassofts SOPHIA CMS
| /zikula/index.php: Zikula CMS
| /system/admin/header.php: Habari Blog
| /system/admin/comments_items.php: Habari Blog
| /scripts/fckeditor/editor/filemanager/connectors/test.html: Digitalus CMS/FCKEditor File upload
| /scripts/fckeditor/editor/filemanager/connectors/uploadtest.html: Digitalus CMS/FCKEditor File upload
| /fckeditor/editor/filemanager/connectors/test.html: phpmotion/FCKEditor File upload
| /fckeditor/editor/filemanager/upload/test.html: Geeklog/FCKEditor File upload
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKEditor File upload
| /fckeditor/editor/filemanager/connectors/php/config.php: DM File Manager/FCKEditor File upload
|
/includes/FCKeditor/editor/filemanager/browser/default/connectors/php/connector.php: PHPNuke/Remote File Download

|
/includes/FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp: PHPnuke/Remote File Download
|
/includes/FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx: PHPnuke/Remote File Download
|
/includes/FCKeditor/editor/filemanager/browser/default/connectors/cfm/connector.cfm: PHPnuke/Remote File Download
|
/includes/FCKeditor/editor/filemanager/browser/default/connectors/lasso/connector.lasso: PHPnuke/Remote File Download
|
/includes/FCKeditor/editor/filemanager/browser/default/connectors/perl/connector.cgi: PHPnuke/Remote File Download
| /includes/FCKeditor/editor/filemanager/browser/default/connectors/py/connector.py: PHPnuke/Remote File Download
| /FCKEditor/editor/filemanager/browser/default/connectors/test.html: EgO or osCMax/FCKeditor File upload
| /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind CMS/FCKeditor File upload
| /Backstage/Components/FreeTextBox/ftb.imagegallery.aspx: Luftguitar CMS/File upload
| /_plugin/fckeditor/editor/filemanager/connectors/test.html: SweetRice/FCKeditor File upload
| /html/news_fckeditor/editor/filemanager/upload/php/upload.php: cardinalCms/FCKeditor File upload
| /fckeditor/editor/filemanager/connectors/test.html: LightNEasy/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /uploadsnaps.php: ZeeMatri/File upload
| /upload/includes/js/files/upload.php: Digital College/File upload
| /tinybrowser/upload.php: Tinybrowser Remote File Upload
| /editor/editor/filemanager/upload/test.html: Tadbir / File Upload
| /photogallery_open.php: Heaven Soft CMS
| /Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx: DotNetNuke / File Upload
| /assetmanager/assetmanager.asp: Asset Manager/Remote File upload
| /Final/login/ava_upl.php: CH-CMS
| /Final/login/ava_upl2.php: CH-CMS
| /spaw/demo.php: SpawCMS/Remote File upload
| /admin/jscript/upload.php: Lizard Cart/Remote File upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
| /admin/jscript/upload.pl: Lizard Cart/Remote File upload
| /admin/jscript/upload.asp: Lizard Cart/Remote File upload
| /databases/acidcat_3.mdb: Acidcat CMS Database
| /mdb-database/dblog.mdb: dBlog Database
| /db/users.mdb: BlogWorx Database
| /infusions/avatar_studio/avatar_studio.php: PHP-Fusion Mod avatar_studio
| /bnnr.php: vBulletin ads_saed
| /vb/bnnr.php: vBulletin ads_saed
| /forum/bnnr.php: vBulletin ads_saed
| /weblink_cat_list.php: WHMCompleteSolution CMS
| /pix/moodlelogo.gif: Moodle files
| /admin/environment.xml: Moodle files
| /typo3/sysext/t3skin/images/login/typo3logo-white-greyback.gif: Typo3 Installation
| /squirrelmail/images/sm_logo.png: SquirrelMail
| /webmail/images/sm_logo.png: SquirrelMail

| /skins/default/images/roundcube_logo.png: RoundCube
| /archive/flash:home/html/images/Cisco_logo.gif: Cisco SDM
| /Default?MAIN=DEVICE: TopAccess Toshiba e-Studio520
| /TopAccess/images/RioGrande/Rio_PPC.gif: TopAccess Toshiba e-Studio520
| /jwsappmngr.jnlp: netForensics
| /nfdesktop.jnlp: netForensics
| /nfservlets/servlet/SPSRouterServlet/: netForensics
| /na_admin/styles/dfm.css: NetworkAppliance NetApp Release 6.5.3P4
| /sitecore/admin/stats.aspx: Sitecore.NET (CMS)
| /sitecore/admin/unlock_admin.aspx: Sitecore.NET (CMS)
| /sitecore/shell/Applications/shell.xml: Sitecore.NET (CMS)
| /sitecore/admin/ShowConfig.aspx: Sitecore.NET (CMS)
| /App_Config/Security/Domains.config.xml: Sitecore.NET (CMS)
| /App_Config/Security/GlobalRoles.config.xml: Sitecore.NET (CMS)
| /sitecore%20modules/staging/service/api.asmx: Sitecore.NET (CMS)
| /sitecore%20modules/staging/workdir: Sitecore.NET (CMS)
|_ /sitecore/system/Settings/Security/Profiles: Sitecore.NET (CMS)
| http-phpmyadmin-dir-traversal:
| VULNERABLE:
| phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2005-3299
| PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the $__redirect parameter, possibly involving the subform array.
|
| Disclosure date: 2005-10-nil
| Extra information:
| ../../../../../etc/passwd not found.
|
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|_ http://www.exploit-db.com/exploits/1244/
9000/tcp open cslistener
MAC Address: EC:71:DB:5F:BA:D6 (Shenzhen Baichuan Digital Technology)

Nmap done: 1 IP address (1 host up) scanned in 161.63 seconds