ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

# Επιχειρησιακό Κέντρο Ασφάλειας για το Διαδίκτυο των Πραγμάτων


**Του φοιτητή**

**Κακλαμάνου Χαραλάμπη**

**Αρ. Μητρώου: 133995**

**Επιβλέπων**

**Δρ. Ηλιούδης Χρήστος**

**Θεσσαλονίκη 2023**

# ΠΡΟΛΟΓΟΣ

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως πτυχιακή εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή Κακλαμάνου Χαραλάμπη που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Διεθνές Πανεπιστήμιο της Ελλάδος άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσίασης στο κοινό και

ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοικτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ’ οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

# ΠΕΡΙΛΗΨΗ

Η άνοδος του Διαδικτύου των Πραγμάτων μας οδήγησε σε μια νέα εποχή τεχνολογίας όπου η πλειοψηφία της έρευνας για το Διαδίκτυο των πραγμάτων επικεντρώνονται στα πρωτόκολλα χαμηλής ενέργειας, στην εξοικονόμηση κόστους, απόδοση και χρηστικότητα. Έρευνα για την ασφάλεια του Διαδικτύου των πραγμάτων αποτελεί τη μειοψηφία του ερευνητικού τομέα. Ο ρόλος ενός Επιχειρησιακού Κέντρου Ασφάλειας για το Διαδίκτυο των Πραγμάτων είναι κρίσιμος. Ένα Επιχειρησιακό Κέντρο Ασφάλειας είναι σαν ένα κέντρο διοίκησης κυβερνοασφάλειας σε έναν οργανισμό. Η κύρια δουλειά του είναι να παρακολουθεί τα δίκτυα και τα συστήματα υπολογιστών του οργανισμού για να εντοπίζει και να ανταποκρίνεται σε τυχόν απειλές ή επιθέσεις στον κυβερνοχώρο. Λειτουργεί ως ομάδα άμυνας, παρακολουθώντας, αναλύοντας και αναλαμβάνοντας δράση για να διατηρήσει τις ψηφιακές πληροφορίες και τα συστήματα ασφαλή από κακόβουλους χρήστες και άλλες αυτοματοποιημένες απειλές. Οι ρόλοι σε ένα Επιχειρησιακό Κέντρο Ασφάλειας απαιτούν τεχνογνωσία όπως και γνώσεις Ασφάλειας Πληροφοριακών Συστημάτων. Ο σκοπός μας είναι να μειώσουμε αυτό το χάσμα. Στην παρούσα εργασία θα χρησιμοποιήσουμε ένα raspberry pi σαν ένα κέντρο διοίκησης και έλεγχου για το Διαδίκτυο των Πραγμάτων και θα υλοποιήσουμε ένα αυτοματοποιημένο σύστημα ανίχνευσης εισβολής. Η επιλογή των λογισμικών που θα γίνει χρήση είναι Ελεύθερο Λογισμικό / Λογισμικό Ανοιχτού Κώδικα.

# ABSTRACT

The rise of the Internet of Things has led us to a new era of technology where the majority of research on the Internet of Things is focused on low-power protocols, cost savings, performance and usability. Research on Internet of Things security is in the minority of the research field. The role of a Security Operation Center for the Internet of Things is critical. A Security Operation Center is like a cybersecurity command center in an organization. Its main job is to monitor the organization's networks and computer systems to detect and respond to any cyber threats or attacks. It acts as a defense team, monitoring, analyzing and taking action to keep digital information and systems safe from malicious users and other automated threats. The roles in a Security Operation Center require expertise as well as knowledge of Information Systems Security. Our goal is to reduce this gap. In this paper we will use a raspberry pi as a command and control center for the Internet of Things and implement an automated intrusion detection system. The choice of software to be used is Free Software/Open Source Software.

ΕΥΧΑΡΙΣΤΙΕΣ

Στην οικογένεια μου για την υπομονή που έδειξαν, και τους καθηγητές μου Ηλιούδη Χρήστο και Χατζημίσιο Περικλή, οι οποίοι με καθοδήγησαν στον τομέα της ασφάλειας και του διαδικτύου των πραγμάτων.

# Κατάλογος περιεχομένων

## Ευρετήριο σχημάτων



Όλες οι καταχωρήσεις του πίνακα Ευρετήριο σχημάτων είναι αποτέλεσμα από στιγμιότυπο οθόνης κατά την εκτέλεση του πειράματος. Δεν λήφθηκαν από το διαδίκτυο και δεν παραβιάζουν άδειες και κανόνες πνευματικών δικαιωμάτων.

Η εικόνα εξωφύλλου κατατάσσεται σε άδεια CC0 (Creative Commons license) ελεύθερη προς χρήση, προαιρετική αναφορά. Η εικόνα λήφθηκε από την

ιστοσελίδα pixahive.com και δημιουργός της εικόνας φέρεται να είναι ο χρήστης Abhinav Thakur.

# ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

IOT → Internet of Things

HTTP → Hypertext tranfer protocol

CVE → Common Vulnerabilities and Exposures

TLS → Transport Layer Security

SSL → Secure Sockets Layer

IEEE → Institute of Electrical and Electronics Engineers

FTP → File Transfer Protocol

SSH → Secure Shell

Dos → Denial of Service

IPS → Intrusion Prevention System

IDS → Intrusion Detection System

GPIO → General Purpose Input Output

Nmap → Network Mapper

SNMP → Simple Network Management Protocol

SMB/CIFS → Server Message Block/Common Internet File

SMTP → Simple Mail Transfer Protocol

UpnP → Universal Plug and Play

ONVIF → Open Network Video Interface Forum

RTMP → Real Time Messaging Protocol

SOC → Security Operations Center

# 1 ΕΙΣΑΓΩΓΗ

Επιχειρησιακό Κέντρο Ασφάλειας ορίζετε μια κεντρική μονάδα ή ομάδα εντός ενός οργανισμού που είναι αφιερωμένη στη διασφάλιση της ασφάλειας των πληροφοριακών συστημάτων, των δεδομένων και της δικτυακής υποδομής του οργανισμού. Κύρια αποστολή του είναι να παρακολουθεί, να ανιχνεύει, να ανταποκρίνεται και να μετριάζει τις απειλές και τα περιστατικά κυβερνοασφάλειας. Στον τομέα της κυβερνοασφάλειας, ένα Επιχειρησιακό Κέντρο Ασφάλειας αποτελεί την καρδιά του οργανισμού για συμβάντα ασφαλείας. Στέκεται σαν βασικός άξονας ο οποίος ενσωματώνει την πρώτη γραμμή άμυνας του οργανισμού ενάντια στις συνεχόμενες απειλές οι οποίες εξελίσσονται στον κυβερνοχώρο.[17] Στον πυρήνα του είναι ένας κεντρικός κόμβος που έχει σχεδιαστεί ώστε να παρακολουθεί, να ανιχνεύει, να ανταποκρίνεται και να μετριάζει απειλές ασφαλείας. Κατέχει κεντρικό ρόλο στην ασφάλεια επιχειρήσεων. Ένα Επιχειρησιακό Κέντρο Ασφαλείας διαθέτει πολλές λειτουργίες. Βασική λειτουργιά του Κέντρου είναι να είναι ένας παρατηρητής ο οποίος με χρήση εργαλείων να παρακολουθεί τις υποδομές, το δίκτυο και τα συστήματα πληροφορικής ενός οργανισμού σε πραγματικό χρόνο.[10] Η συνεχής παρακολούθηση αποτελεί την βάση ώστε να γίνει ανίχνευση των ασυνήθιστων συμπεριφορών ή συμβάντων ασφαλείας. Με τον εντοπισμό μίας πιθανής απειλής, το Κέντρο Ασφαλείας μεταβαίνει σε δράση ώστε να αντιμετωπισθεί το συμβάν. Η ταχεία αντίδραση είναι υψίστης σημασίας σε περίπτωση συμβάντος ασφαλείας. Οι αναλυτές ασφαλείας του Κέντρου αναλύουν και μετριάζουν τις απειλές ώστε να γίνει αποτελεσματικά η ελαχιστοποίηση πιθανών ζημιών.[9] Το Κέντρο Ασφαλείας τροφοδοτείτε με πληροφορίες από τις απειλές οι οποίες εξετάζονται. Αξιοποιώντας διάφορες πηγές από εσωτερικές αναλύσεις δεδομένων το Κέντρο Ασφαλείας παραμένει ενήμερο για πρόσφατες απειλές στον τομέα της κυβερνοασφάλειας, τεχνικές επιθέσεων, γνωστές ευπάθειες. Αυτός είναι ο τρόπος με τον οποίο το Κέντρο Ασφαλείας προσεγγίζει προληπτικά απειλές. Η οργάνωση του Κέντρου Ασφαλείας αποτελείται από διαφορετικές ομάδες και ρόλους.[10] Οι αναλυτές ασφαλείας, ανταποκριτές συμβάντων, αναλυτές πληροφοριών και διαχειριστές του Κέντρου είναι σε συνεχή επικοινωνία και συνεργασία ώστε να πετύχουν μια ισχυρή άμυνα στις απειλές τις οποίες αντιμετωπίζει το Κέντρο Ασφαλείας. Η τεχνολογική υποδομή του Κέντρου αποτελείται από το Σύστημα Ασφαλείας Πληροφοριών και Διαχείρισης Συμβάντων το οποίο συγκεντρώνει και αναλύει δεδομένα καταγραφής ώστε να εντοπίσει μοτίβα και ανωμαλίες.[9] Συστήματα ανίχνευσης εισβολής όπως και συστήματα αποτροπής εισβολής έχουν σημαντικό ρόλο στον εντοπισμό και την πρόληψη κακόβουλων ή ύποπτων δραστηριοτήτων στο δίκτυο. Η εξέλιξη του Κέντρου Ασφαλείας είναι αυτή που το καθορίζει σημαντικό. Είναι μια εξέλιξη στον τομέα της

κυβερνοασφάλειας. Τα Επιχειρησιακά Κέντρα Ασφαλείας εστίαζαν στην άμεση αντίδραση των περιστατικών κατά την εκδήλωσή τους. Για να κατανοήσουμε την σημαντικότητα και την αναγκαιότητα ενός Επιχειρησιακού Κέντρου Ασφαλείας θα πρέπει να το αντιλαμβανόμαστε ως απάντηση στην συχνότητα των απειλών στον κυβερνοχώρο. Η προληπτική στάση η οποία κρατάνε τα Κέντρα Ασφαλείας ενσωματώνει αυτοματοποίηση, ανάλυση απειλών, εντοπισμό και μετριασμό των απειλών πριν κλιμακωθούν.[17] Η σημασία ενός Κέντρου Ασφαλείας στους σύγχρονους οργανισμούς είναι κρίσιμη. Διαδραματίζει καθοριστικό ρόλο στον μετριασμό των κινδύνων. Με τον προληπτικό εντοπισμό και την αντιμετώπιση πιθανών απειλών ασφαλείας, βοηθά τους οργανισμούς να ελαχιστοποιήσουν τις επιπτώσεις από τα περιστατικά ασφαλείας, διαφυλάσσει την ακεραιότητα των ευαίσθητων δεδομένων και την ακεραιότητα των συστημάτων. Το Κέντρο Ασφαλείας είναι καθοριστικό για την διασφάλιση της συμμόρφωσης με κανόνες ασφαλείας. Πολλοί κλάδοι και περιοχές έχουν εφαρμόσει ισχυρά κανονιστικά πλαίσια και ένα Κέντρο Ασφαλείας αποδεικνύει τη δέσμευση ενός οργανισμού για την ασφάλεια στον κυβερνοχώρο, τη συμμόρφωση και την προστασία των δεδομένων. Η αποτελεσματικότητα στην αντιμετώπιση περιστατικών είναι ένα χαρακτηριστικό ενός καλά δομημένου Κέντρου Ασφαλείας. Η ταχεία αντίδραση σε περιστατικά ασφαλείας είναι ζωτικής σημασίας. Ελαχιστοποιεί τον χρόνο διακοπής λειτουργίας, τον περιορισμό των παραβιάσεων και την διατήρηση της λειτουργικής ακεραιότητας των πόρων ενός οργανισμού.[9] Με την άνοδο του Διαδικτύου των Πραγμάτων οι έξυπνες πόλεις έρχονται καθημερινά πιο κοντά στην ζωή μας. Μία έξυπνη πόλη παρέχει όμως προκλήσεις ασφάλειας οι οποίες θα λυθούν και θα αντιμετωπισθούν από ένα Επιχειρησιακό Κέντρο Ασφαλείας. Καθώς οι έξυπνες πόλεις συνεχίζουν να εξελίσσονται, ενσωματώνοντας προηγμένες τεχνολογίες και διασυνδεδεμένα συστήματα, η ανάγκη για υλοποίηση ενός Κέντρου Ασφαλείας είναι ύψιστης σημασίας. Οι έξυπνες πόλεις βασίζονται σε μεγάλο βαθμό σε διασυνδεδεμένες κρίσιμες υποδομές, συμπεριλαμβανομένων των συστημάτων μεταφορών, των ενεργειακών δικτύων και των δικτύων επικοινωνίας. Τα συστήματα αυτά είναι ευάλωτα σε επιθέσεις.[20] Η αύξηση από επιθέσεις Ransomware το 2023 είναι 95% σε σχέση με το 2022.[8] Ένα Κέντρο Επιχειρήσεων Ασφαλείας μπορεί να παρέχει συνεχή παρακολούθηση και προληπτική ανίχνευση απειλών, αποτρέποντας και μετριάζοντας πιθανές επιθέσεις σε υποδομές ζωτικής σημασίας. Οι έξυπνες πόλεις συλλέγουν τεράστιες ποσότητες δεδομένων από αισθητήρες, κάμερες παρακολούθησης και διάφορες συσκευές IoT για τη βελτίωση των υπηρεσιών και του αστικού σχεδιασμού. Ωστόσο, αυτά τα δεδομένα εγείρουν επίσης ανησυχίες σχετικά με το απόρρητο και την ασφάλεια των πολιτών. Το Κέντρο Ασφαλείας εφαρμόζει ισχυρά μέτρα προστασίας δεδομένων, διασφαλίζοντας ότι ο χειρισμός ευαίσθητων πληροφοριών

γίνεται με ασφάλεια. Η υλοποίηση ενός Επιχειρησιακού Κέντρου Ασφαλείας σε μια έξυπνη πόλη όμως δεν αντιμετωπίζει τις προκλήσεις που υπάρχουν και παρέχει λύσεις απλά, παρέχει εμπιστοσύνη στην πόλη.[21] Η διασφάλιση της εμπιστοσύνης είναι ένα κρίσιμο στοιχείο στην υλοποίηση όλων των έργων. Οι ειδήσεις για παραβιάσεις ασφάλειας ή διαρροές δεδομένων μπορούν να διαβρώσουν την εμπιστοσύνη στην ικανότητα της πόλης να προστατεύει τους πολίτες της. Ένα Επιχειρησιακό Κέντρο Ασφάλειας συμβάλλει ενεργά στην οικοδόμηση και διατήρηση της εμπιστοσύνης των πολιτών.

## *1.1 Στόχοι Πτυχιακής Εργασίας*

Οι στόχοι της παρούσας πτυχιακής εργασίας είναι να αναδείξει τον κεντρικό ρόλο του Επιχειρησιακού Κέντρου Ασφαλείας ώστε να ενισχύσει την ασφάλεια σε μία έξυπνη πόλη, με έμφαση στην ενσωμάτωση του Διαδικτύου των Πραγμάτων με χρήση Συστημάτων Ανίχνευσης Εισβολής. Εμβαθύνοντας στον τρόπο λειτουργίας των κανόνων ενός Συστήματος Ανίχνευσης Εισβολής και αναλύοντας επιθέσεις κυβερνοασφάλειας. Το πειραματικό σκέλος υλοποιεί επίθεση σε ένα Raspberry Pi το οποίο προσομοιώνει έναν κόμβο του Διαδικτύου των Πραγμάτων και στην συνέχεια θα μπορούσε να είναι ένας σημαντικός κόμβος σε μία έξυπνη πόλη σε κάποιον τομέα διαχείρισης. Αναλύοντας την επίθεση ώστε να γίνει δημιουργία ενός κανόνα μπορούμε να δούμε την κρισιμότητα μίας επίθεσης σε βάθος και πόσο σημαντικό είναι να υπάρχουν προληπτικά μέτρα ασφάλειας τα οποία μας διευκολύνουν στην αναγνώριση του περιστατικού.

## *1.2 Επιτεύγματα*

Με την υλοποίηση της παρούσας πτυχιακής εργασίας, βρισκόμαστε σε θέση να εφαρμόσουμε μεθοδολογίες άμυνας οι οποίες χρησιμοποιούνται από ένα Κέντρο Ασφαλείας. Να εξοικειωθούμε με τα εργαλεία και τους αντίστοιχους ρόλους του Κέντρου, να αναλύσουμε επιθέσεις σε επίπεδο δικτύου και να δημιουργήσουμε δικούς μας κανόνες προς υλοποίηση. Εξοικειωνόμαστε με το Κέντρο Ασφαλείας και το Διαδίκτυο των Πραγμάτων, και εστιάζουμε στον ρόλο της ασφάλειας σε μία έξυπνη πόλη. Με την ολοκλήρωση του πειραματικού σκέλους μπορούμε να χρησιμοποιήσουμε ένα Raspberry Pi ώστε να προστατεύσουμε το προσωπικό μας

δίκτυο σε ένα έξυπνο σπίτι στο οποίο είναι συνδεμένες έξυπνες συσκευές όπως μία έξυπνη τηλεόραση, έξυπνη κάμερα και κατά επέκταση σε μία έξυπνη πόλη.

## *1.3 Διάρθρωση Πτυχιακής Εργασίας*

Στον κόσμο ο οποίος οδεύει στο Διαδίκτυο των Πραγμάτων η κυβερνοασφάλεια έχει κρίσιμη σημασία. Η παρούσα πτυχιακή εργασία καλύπτει τον βασικό ρόλο ενός Κέντρου Επιχειρήσεων Ασφαλείας στο Διαδίκτυο των Πραγμάτων. Ένα Κέντρο Επιχειρήσεων Ασφαλείας είναι υπεύθυνο για την παρακολούθηση, τον εντοπισμό και την απόκριση σε απειλές στον κυβερνοχώρο, την προστασία κρίσιμων περιουσιακών στοιχείων και δεδομένων. Το Διαδίκτυο των Πραγμάτων εισάγει προκλήσεις σε θέματα ασφαλείας τα οποία συμπεριλαμβάνουν τρωτά σημεία για επιθέσεις μεγάλης κλίμακας. Ένα Σύστημα Ανίχνευσης Εισβολής έχει σημαντικό ρόλο στην άμυνα, παρακολουθώντας την κυκλοφορία του δικτύου για ύποπτες δραστηριότητες και γνωστά μοτίβα των επιθέσεων. Στο πρακτικό σκέλος της πτυχιακής εργασίας με την χρήση του Snort το οποίο είναι ένα Σύστημα Ανίχνευσης Εισβολής ανοιχτού κώδικα / ελεύθερου λογισμικού, θέτουμε και δημιουργούμε κανόνες για την αντιμετωπίσει επιθέσεων μετά από ανάλυση του δικτύου με το Wireshark. Η αποτελεσματικότητα της άμυνας και η ανάλυση της κυκλοφορίας του δικτύου με εργαλεία ανοιχτού κώδικα παρέχουν μια στιβαρή αρχή προς την επέκταση της υλοποίηση του Κέντρου Ασφαλείας σε μία έξυπνη πόλη, και την καθιέρωση προτύπων και μέτρων ασφαλείας σε μελλοντικές τεχνολογίες και υλοποιήσεις.

# 2 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΚΕΝΤΡΟ ΑΣΦΑΛΕΙΑΣ

## *2.1 Τμήματα Κέντρου Ασφάλειας*

- **Αναλυτές**: Οι αναλυτές είναι ο πυρήνας της ομάδας. Παρακολουθούν τις ειδοποιήσεις ασφάλειας, διερευνούν περιστατικά και αναλαμβάνουν δράση για τον μετριασμό των απειλών. Οι αναλυτές μπορούν να κατηγοριοποιηθούν σε διαφορετικά επίπεδα βάση γνώσεων και εμπειρίας. Η εξειδίκευση σε μεμονωμένα περιστατικά όπως ανάλυση κακόβουλου λογισμικού ή περιστατικά πλημμύρας όπου το κέντρο λαμβάνει συνεχώς ειδοποιήσεις για περιστατικά είναι βασικά κριτήρια για αναλυτές μεγάλου επιπέδου. Συχνό αλλά όχι υποχρεωτικό χαρακτηριστικό των αναλυτών, είναι η εργασία με βάρδιες ώστε να υπάρχει συνεχόμενη κάλυψη των περιστατικών.[10]
- **Ομάδα Αντιμετώπισης Συμβάντων**: Αυτή η ομάδα ειδικεύεται στην ανταπόκριση και διαχείριση περιστατικών κυβερνοασφάλειας. Διερευνούν τις παραβιάσεις της ασφάλειας, συντονίζουν τις προσπάθειες αντιμετώπισης περιστατικών και εργάζονται για τον περιορισμό και τον μετριασμό των επιπτώσεων των περιστατικών.[10]
- **Κυνηγοί Απειλών**: Εξειδικευμένοι αναλυτές οι οποίοι αναζητούν και εντοπίζουν προληπτικά προηγμένες απειλές και ανωμαλίες που ενδέχεται να μην ανιχνεύονται από αυτοματοποιημένα εργαλεία ασφαλείας. Οι κυνηγοί απειλών χρησιμοποιούν προηγμένες τεχνικές και πληροφορίες απειλών για να ανακαλύψουν κρυφές απειλές.[10]
- **Μηχανικοί ασφάλειας**: Οι μηχανικοί ασφαλείας σχεδιάζουν, εφαρμόζουν και διατηρούν την υποδομή και τις τεχνολογίες ασφαλείας που χρησιμοποιούνται στο Κέντρο Ασφάλειας. Διασφαλίζουν ότι τα εργαλεία ασφαλείας είναι σωστά διαμορφωμένα και ενημερωμένα.[10]
- **Ομάδα διαχείρισης ευπάθειας**: Αυτή η ομάδα εστιάζει στον εντοπισμό και την αποκατάσταση ευάλωτων σημείων στα συστήματα και τις εφαρμογές του οργανισμού. Διενεργούν αξιολογήσεις ευπάθειας, δίνουν προτεραιότητα στις προσπάθειες αποκατάστασης και διασφαλίζουν ότι τα συστήματα είναι ενημερωμένα με ενημερώσεις κώδικα.[9]

- **Αναλυτές πληροφοριών απειλών**: Οι αναλυτές πληροφοριών απειλών συλλέγουν και αναλύουν πληροφορίες σχετικά με τρέχουσες και αναδυόμενες απειλές στον κυβερνοχώρο.[9]
- **Αρχιτέκτονες ασφάλειας**: Οι αρχιτέκτονες ασφάλειας σχεδιάζουν τη συνολική αρχιτεκτονική ασφάλειας του οργανισμού. Ο συγκεκριμένος ρόλος είναι ρόλος υψίστης ευθύνης και αναλαμβάνετε από επαγγελματίες ασφάλειας οι οποίοι έχουν μεγάλο επίπεδο εμπειρίας. Συνεργάζονται με όλες τις ομάδες από τα τμήματα του επιχειρησιακού κέντρου ασφάλειας για την εφαρμογή μέτρων ασφαλείας.[17]
- **Ειδικοί Συμμόρφωσης και Πολιτικής**: Αυτοί οι ειδικοί διασφαλίζουν ότι ο οργανισμός συμμορφώνεται με τις κανονιστικές απαιτήσεις και τις πολιτικές εσωτερικής ασφάλειας. Βοηθούν στον έλεγχο και την υποβολή εκθέσεων σχετικά με τα μέτρα ασφαλείας.[9]
- **Ιατροδικαστικοί αναλυτές**: Οι συγκεκριμένοι αναλυτές ειδικεύονται στην ψηφιακή εγκληματολογία και την έρευνα. Συλλέγουν και αναλύουν ψηφιακά στοιχεία σε περίπτωση περιστατικού ασφαλείας ή παραβίασης.[9]
- **Ομάδα ευαισθητοποίησης και εκπαίδευσης για θέματα ασφάλειας**: Είναι υπεύθυνη για την εκπαίδευση των εργαζομένων και των χρηστών σχετικά με τις βέλτιστες πρακτικές ασφάλειας και την ευαισθητοποίηση σχετικά με πιθανές απειλές. Η συγκεκριμένη ομάδα είναι υπεύθυνη για ελεγχόμενες καμπάνιες επιθέσεων ‘ψαρέματος’ στα μέλη άλλων ομάδων. [17]
- **Διαχειριστές δικτύου και συστημάτων**: Οι διαχειριστές δικτύου και συστημάτων παρέχουν υποστήριξη για εργαλεία ασφαλείας, διατηρούν αρχεία καταγραφής συστήματος και συνεργάζονται με το Κέντρο ασφάλειας σε εργασίες που σχετίζονται με την ασφάλεια.[17]
- **Νομικοί σύμβουλοι και σύμβουλοι συμμόρφωσης**: Οι νομικοί και οι ειδικοί σε θέματα συμμόρφωσης διασφαλίζουν ότι οι δραστηριότητες του Κέντρου ασφάλειας ευθυγραμμίζονται με τις νομικές και κανονιστικές απαιτήσεις.[17]
- **Ομάδα Διαχείρισης Κινδύνων**: Υπεύθυνη για την αξιολόγηση και τη διαχείριση κινδύνων κυβερνοασφάλειας, τη διεξαγωγή αξιολογήσεων κινδύνου, την ιεράρχηση των προσπαθειών μετριασμού και την ανάπτυξη πολιτικών ασφάλειας για την ευθυγράμμιση με την ανοχή κινδύνου και τους επιχειρηματικούς στόχους του οργανισμού.[10]

## *2.2 Ροή εργασιών κέντρου*

Ακολουθεί η ροή εργασίας ενός Κέντρου ασφάλειας χωρίς Ενορχήστρωση ασφάλειας, αυτοματοποίηση και απόκριση.[17]

I. Δημιουργία ειδοποιήσεων
    1. Η ροή εργασίας ξεκινά με τη δημιουργία ειδοποιήσεων ασφάλειας από διάφορες πηγές.
    2. Οι αναλυτές είναι οι πρώτοι που λαμβάνουν την ειδοποίηση.

II. Διαλογή ειδοποίησης
    1. Οι αναλυτές καθορίζουν την σοβαρότητα και την εγκυρότητα των ειδοποιήσεων.
    2. Αξιολογούν εάν μια ειδοποίηση είναι αληθινό περιστατικό ασφάλειας ή ψευδώς θετικό.
    3. Με βάση την ανάλυση, οι ειδοποιήσεις ταξινομούνται και κατατάσσονται σε ιεραρχία.

III. Διερεύνηση περιστατικού
    1. Εάν μια ειδοποίηση επιβεβαιωθεί ως περιστατικό ασφαλείας, προωθείται σε αναλυτή υψηλότερου επιπέδου για περαιτέρω έρευνα.
    2. Ο αναλυτής συλλέγει πρόσθετα δεδομένα ώστε να εξετάσει το συμβάν σε βάθος.
    3. Σκοπός τις διερεύνησης είναι να καθοριστεί το εύρος του περιστατικού όπως και το αντίκτυπο.

IV. Περιορισμός και μετριασμός
    1. Αφού προσδιορίσουν τη φύση και την έκταση του περιστατικού, οι αναλυτές λαμβάνουν μέτρα για τον περιορισμό της απειλής και την ελάττωση των επιπτώσεων.
    2. Η απομόνωση συστημάτων που επηρεάστηκαν, αλλαγή στοιχείων ελέγχου πρόσβαση είναι μέτρα τα οποία εφαρμόζουν οι αναλυτές.

V. Συνεργασία και κλιμάκωση
    1. Εάν είναι απαραίτητο, τα περιστατικά μπορεί να κλιμακωθούν σε αναλυτές υψηλότερου επιπέδου ξανά. Επίσης εάν κριθεί αναγκαίο η

κλιμάκωση μπορεί να περιλαμβάνει εξειδικευμένες ομάδες όπως η ομάδα αντιμετώπισης συμβάντων ή η ομάδα κυνηγιού απειλών.

2. Σε αυτό το στάδιο μπορεί να προκύψει συνεργασία με άλλες ομάδες εντός του κέντρου ασφάλειας, καθώς με τα εξωτερικά μέρη, όπως αρχές επιβολής του νόμου.

VI. Αποκατάσταση

1. Οι ομάδες του κέντρου ασφάλειας εργάζονται για την αποκατάσταση της βασικής αιτίας του συμβάντος. Αυτό μπορεί να περιλαμβάνει επιδιόρθωση ευπαθειών, ενημέρωση λογισμικού και βελτίωση των μέτρων ασφάλειας.
2. Βασικός στόχος είναι να αποτρέψουν παρόμοια περιστατικά στο μέλλον.

VII. Αναφορά

1. Σε όλη την διάρκεια της ροής εργασιών, οι αναλυτές διατηρούν λεπτομερή αρχεία του περιστατικού, συμπεριλαμβάνοντας το χρονοδιάγραμμα των γεγονότων και των ενεργειών που πραγματοποιήθηκαν.
2. Οι αναφορές περιστατικών είναι κρίσιμες για τον έλεγχο και την ανάλυση μετά το συμβάν. Σε σενάρια τα οποία το κέντρο ασφάλειας παρέχει υπηρεσίες σε έναν πελάτη η αναφορά είναι το τεκμήριο το οποίο θα σταλεί στον πελάτη.

VIII. Συνεχής Παρακολούθηση

1. Ακόμη και μετά την επίλυση ενός περιστατικού, οι ομάδες του κέντρου ασφάλειας συνεχίζουν να παρακολουθούν το περιβάλλον.
2. Η συνεχής παρακολούθηση βοηθά ώστε να διασφαλιστεί πως ο οργανισμός παραμένει ασφαλής.

IX. Ανάλυση και ανατροφοδότηση

1. Οι ομάδες αναλύουν δεδομένα περιστατικών ώστε να εντοπίσουν τάσεις, πρότυπα και τομείς προς βελτίωση.

X. Εκπαίδευση

1. Οι αναλυτές λαμβάνουν συνεχή εκπαίδευση για να παραμένουν ενημερωμένοι με τις πιο πρόσφατες απειλές και τεχνολογίες για την ασφάλεια.

2. Η ενημέρωση για θέματα ασφαλείας είναι κρίσιμη ώστε να μπορεί το κέντρο ασφάλειας να ανταποκρίνεται σε καινούριες απειλές.[17]

## *2.3 Διαχείριση Πληροφοριών Ασφαλείας και Συμβάντων*

Η διαχείριση πληροφοριών ασφάλειας και συμβάντων είναι ένα συνδυαστικό σύστημα στην διαχείριση πληροφοριών ασφάλειας και διαχείριση συμβάντων. Το σύστημα συλλέγει, αναλύει και συγκρίνει δεδομένα από διάφορες πηγές. Η συλλογή δεδομένων γίνετε από πηγές στο δίκτυο ενός οργανισμού συμπεριλαμβανομένου και των συσκευών ασφάλειας όπως ένα τείχος προστασίας ή συστήματα ανίχνευσης εισβολών. Τα δεδομένα που συλλέγονται περιλαμβάνουν αρχεία καταγραφής, συμβάντα και πληροφορίες που σχετίζονται με την ασφάλεια. [21] Η διαχείριση και η αποθήκευση των αρχείων καταγραφής συγκεντρώνονται. Τα αρχεία καταγραφής δημιουργούνται από διάφορες συσκευές καθώς εκτελούν τις λειτουργίες τους. Βασική βοήθεια της διαχείρισης πληροφοριών ασφάλειας και συμβάντων είναι η οργάνωση και αποθήκευση των δεδομένων προς ανάλυση. Η παρακολούθηση γίνετε σε πραγματικό χρόνο ώστε να υπάρχει συνεχής παρακολούθηση και να μην χάνονται δεδομένα. Αναλύουν εισερχόμενα δεδομένα ώστε να εντοπιστούν περιστατικά ασφάλειας ή ανωμαλίες που δηλώνουν πιθανή απειλή στο σύστημα. Γίνετε συσχέτιση συμβάντων και δεδομένων από πολλαπλές πηγές, βασικός στόχος είναι η αναζήτηση από μοτίβα, αλληλουχίες γεγονότων, τα οποία μεμονωμένα μπορεί να μην φαίνονται κακόβουλα αλλά συνδυαστικά υποδεικνύουν περιστατικά ασφάλειας. Δυο λάθος προσπάθειες πρόσβασης μεμονωμένα δεν είναι κακόβουλο συμβάν ασφάλειας, αλλά σε συνδυασμό τον χρόνο των αιτημάτων και την τοποθεσία μπορεί να κατατάσσονται σε επίθεση λεξικού ή ανωμαλία πρόσβασης.[10] Με τον εντοπισμό ύποπτης ή ανώμαλης δραστηριότητας, δημιουργεί ειδοποιήσεις. Αυτές είναι οι ειδοποιήσεις οι οποίες αποστέλλονται στους αναλυτές ασφάλειας ή στους διαχειριστές ώστε να γίνει διερεύνηση. Η παρακολούθηση επίσης εκτίνετε και στην δραστηριότητα των χρηστών ώστε να εντοπιστούν παραβιάσεις. Σε περίπτωση συμβάντος ασφάλειας, η διαχείριση πληροφοριών ασφάλειας παρέχει λεπτομερή δεδομένα και αρχεία καταγραφής ώστε να μπορέσει να υλοποιηθεί ψηφιακή εγκληματολογία και ανάλυση των αιτιών.[9]

## *2.4 Ενορχήστρωση Αυτοματοποίηση και Απόκριση Ασφάλειας*

Η Ενορχήστρωση Αυτοματοποίηση και Απόκριση Ασφάλειας είναι μια τεχνική προσέγγιση στις λύσεις που προσφέρει το κέντρο ασφάλειας. Οι δυνατότητα αυτοματισμού παρέχει βέλτιστες λύσεις και η ενορχήστρωση βελτιώνει την διαχείριση ασφάλειας του κέντρου.[17]

1. Ενορχήστρωση: Συνδέει διαφορετικά εργαλεία και συστήματα ασφάλειας.
2. Αυτοματισμός: Αναλαμβάνει την υλοποίηση επαναλαμβανόμενων εργασιών με σκοπό να μειώσει τον φόρτο εργασίας των αναλυτών. Οι αναλυτές μπορούν να αφιερώσουν ποιοτικό χρόνο σε σημαντικές εργασίες.
3. Βιβλία σχεδίου: Τα βιβλία σχεδίου δρουν σαν οδηγοί ανάλογα το συμβάν ώστε να υπάρχει άμεση αντίδραση από τους αναλυτές. Τα βιβλία σχεδίου δημιουργούν μια ροή και εκτελούν αυτοματισμούς σε κάθε ολοκληρωμένο στάδιο. Ανάλογα την υλοποίηση του συστήματος μπορούν να υπάρχουν κατά σειρά πολλαπλά βιβλία σχεδίου. Βασικός σκοπός της χρήσης βιβλίων σχεδίου είναι τα περιστατικά να αντιμετωπίζονται με δομημένο τρόπο.
4. Ενσωμάτωση: Δρα σαν κεντρικός κόμβος για τις λειτουργίες ασφάλειας.
5. Εμπλουτισμός Δεδομένων: Πληροφορίες σχετικές με το περιστατικό εμπλουτίζονται στις ειδοποιήσεις. Ένα κρίσιμο χαρακτηριστικό σε τεχνικές ασφάλειας οι οποίες απαιτούν τεχνογνωσία είναι να μπορούν να διευκολύνουν αναλυτές χαμηλού επιπέδου ώστε να κατανοούν και να μπορούν να δράσουν σε περιστατικά μεγαλύτερου βαθμού.
6. Αναφορά: Το σύστημα στέλνει ειδοποιήσεις όταν υπάρχει περιστατικό και παρέχει λεπτομερή αναφορά για την υγεία του συστήματος, ώστε να διασφαλίζετε η ομαλή λειτουργία του.
7. Παρακολούθηση: Το σύστημα παρακολουθεί και διαχειρίζεται τα περιστατικά ασφάλειας από την αρχή έως την επίλυση. Γίνετε διασφάλιση σε κάθε βήμα των διαδικασιών πως η απόκριση στο συμβάν τεκμηριώνεται και καταγράφετε.

Η Διαχείριση Πληροφοριών Ασφάλειας και Συμβάντων με την Ενορχήστρωση Αυτοματοποίηση και Απόκριση Ασφάλειας έχουν πολλά κοινά στοιχεία. Οι ρόλοι όμως διαφέρουν γιατί η Διαχείριση Πληροφοριών Ασφάλειας είναι υπεύθυνη για

την παρακολούθηση και την ειδοποίηση, ενώ η Ενορχήστρωση Αυτοματοποίηση για τους αυτοματισμούς και την απόκριση στα ζητήματα ασφάλειας.

Ο συνδυασμός των ομάδων των αναλυτών, τεχνολογιών Ανίχνευσης Εισβολής, Διαχείρισης Πληροφοριών Ασφαλείας και Συμβάντων μαζί με Ενορχήστρωση Αυτοματοποίηση και Απόκριση Ασφαλείας μας παρέχει μία ολιστική προσέγγιση για την ασφάλεια στον κυβερνοχώρο. Τα στοιχεία του Κέντρου Ασφαλείας συνεργάζονται για να παρέχουν την προληπτική άμυνα, επιτρέποντας στο Κέντρο να παρακολουθεί, να εντοπίζει και να ανταποκρίνεται αποτελεσματικά ακόμα και σε καινούριες απειλές μηδενικής μέρας. Η ενσωμάτωση ανθρώπινης τεχνογνωσίας και ανεπτυγμένων εργαλείων διασφαλίζει την ισορροπία στην προσέγγιση για την αντιμετώπιση απειλών στον τομέα της ασφαλείας. Οι ομάδες συνεργάζονται ώστε να δημιουργήσουν ένα ολοκληρωμένο πλαίσιο ασφαλείας το οποίο μπορεί να εντοπίζει και να ανταποκρίνεται στις απειλές στον κυβερνοχώρο βέλτιστα. Οι ομάδα των αναλυτών είναι εξειδικευμένοι στον τομέα παρακολούθησης των ειδοποιήσεων ασφαλείας και την ανάλυση δεδομένων. Οι ομάδα αντιμετώπισης περιστατικών παρέχει λύσεις οι οποίες εστιάζουν στον χειρισμό και τον μετριασμό ενός περιστατικού ασφαλείας. Σε συνδυασμό με τις τεχνολογίες Διαχείρισης Πληροφοριών Ασφαλείας και Συμβάντων και τα Συστήματα Ανίχνευσης Εισβολής, ένα Επιχειρησιακό Κέντρο Ασφαλείας είναι σε θέση να παρέχει μία σφαιρική εικόνα προς τις απειλές τις οποίες αντιμετωπίζει καθημερινά ο χώρος της κυβερνοασφάλειας.[17]

# 3 ΔΙΑΔΥΚΤΙΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

## ΕΙΣΑΓΩΓΗ

Το διαδίκτυο των πραγμάτων, αντιπροσωπεύει μια τεχνολογική επανάσταση όπου καθημερινά αντικείμενα είναι εξοπλισμένα με αισθητήρες και συνδεσιμότητα στο Διαδίκτυο. Αυτές οι διασυνδεμένες συσκευές μπορούν να συλλέγουν και να μοιράζονται δεδομένα, επιτρέποντας την αυτοματοποίηση και την βελτίωση της απόδοσης σε διαφορετικούς τομείς. Οι εφαρμογές του Διαδικτύου των Πραγμάτων εκτείνονται από έξυπνα σπίτια μέχρι τον βιομηχανικό αυτοματισμό και την υγειονομική περίθαλψη.[29] Ένα κρίσιμο χαρακτηριστικό στον τομέα της Ασφάλειας είναι πως οτιδήποτε διαθέτει πρόσβαση στο διαδίκτυο μπορεί να αποτελέσει στόχο από κακόβουλους χρήστες ή αυτοματοποιημένο λογισμικό. Αναλυτικά θα εμβαθύνουμε στα πιο συχνά πρωτόκολλα τα οποία υλοποιούνται το Διαδίκτυο των Πραγμάτων. Το Διαδίκτυο των Πραγμάτων αποτελεί δομή για την υλοποίηση μίας Έξυπνης Πόλης. Η έννοια της Έξυπνης Πόλης είναι μια αλλαγή η οποία αξιοποιώντας την δύναμη του Διαδικτύου των Πραγμάτων, ενισχύει την αποτελεσματικότητα της και την ποιότητα ζωής των κατοίκων της. Μια έξυπνη πόλη ενσωματώνει προηγμένες τεχνολογίες για την συλλογή και ανάλυση δεδομένων, επιτρέποντας την έξυπνη λήψη αποφάσεων και την διαχείριση. Αυτή η συλλογή δεδομένων έρχεται σε αρμονία με την συλλογή δεδομένων του Επιχειρησιακού Κέντρου Ασφαλείας. Μια Έξυπνη Πόλη χαρακτηρίζεται από τη διασυνδεδεμένη υποδομή της, όπου τα διάφορα στοιχεία επικοινωνούν για τη δημιουργία ενός δυναμικού και αποτελεσματικού περιβάλλοντος. Δίνει προτεραιότητα στις αποτελεσματικές και βιώσιμες μεταφορές. Η διαχείριση της κυκλοφορίας με την χρήση συσκευών του Διαδικτύου των Πραγμάτων, έξυπνες λύσεις για την στάθμευσή και ενημέρωση των δημόσιων συγκοινωνιών σε πραγματικό χρόνο συμβάλλουν στην ομαλότερη ροή της κυκλοφορίας και στην μείωση της κυκλοφοριακής συμφόρησης.[12] Οι συσκευές Διαδικτύου των Πραγμάτων αποτελούν τον κορμό της Έξυπνης Πόλης, είναι τοποθετημένες στρατηγικά σε σημεία ώστε να αναλύουν δεδομένα για την λήψη αποφάσεων. Αισθητήρες και ενεργοποιητές παρατηρούν και καταγράφουν δεδομένα για πάντα, από την κυκλοφορία και την κατανάλωση ενέργειας έως τις περιβαλλοντικές συνθήκες. Η ανάλυση αυτών των δεδομένων ωθεί τις Έξυπνες Πόλεις στην ανάπτυξή. Τεράστια σύνολα δεδομένων που δημιουργούνται από τις συσκευές αποθηκεύονται, όπου εξελιγμένες πλατφόρμες αναλυτικών στοιχείων εξετάζουν το θόρυβο, εξάγοντας χρήσιμες πληροφορίες.[20]

## *3.1 MQTT*

Το MQTT (Message Queuing Telemetry Transport) είναι βασικό πρωτόκολλο ανταλλαγής μηνυμάτων. Η χρησιμότητα του είναι ιδιαίτερη στο πλαίσιο του Διαδικτύου των Πραγμάτων. Η αρχιτεκτονική του στηρίζετε σε τρία στοιχεία εκδότες, συνδρομητές και έναν κεντρικό διαμεσολαβητή. Οι εκδότες είναι συσκευές ή εφαρμογές που δημιουργούν μηνύματα και θέλουν να τα μοιραστούν. Οι εκδότες στέλνουν τα μηνύματα στο διαμεσολαβητή για διανομή. Οι συνδρομητές δηλώνουν ενδιαφέρον για συγκεκριμένα θέματα και λαμβάνουν μηνύματα που σχετίζονται με αυτά τα θέματα. Εγγράφονται ανάλογά τα θέματα ενδιαφέροντος στον διαμεσολαβητή. Ο Διαμεσολαβητής είναι ο κεντρικός διακομιστής. Λαμβάνει όλα τα μηνύματα από τους εκδότες και τα προωθεί στους κατάλληλους συνδρομητές με βάση τις συνδρομές τους στο θέμα. Τα μηνύματα του MQTT στέλνονται χωρίς κρυπτογραφία. Η ασφάλιση των μηνυμάτων γίνετε μέσω της χρήσης εξωτερικών μηχανισμών ασφάλειας και πρωτοκόλλων. Τα πρωτόκολλα Transport Layer Security και Secure Sockets Layer είναι αυτά που χρησιμοποιούνται για την προστασία της επικοινωνίας. Το πρωτόκολλο Secure Sockets Layer, είναι ενα κρυπτογραφικό πρωτόκολλο το οποίο σχεδιάστηκε για την ασφαλή μετάδοση δεδομένων μέσω δικτύων υπολογιστών. Το πρωτόκολλο Transport Layer Security είναι η αναβάθμιση όπου υλοποιήθηκε ώστε να διορθώσει ευπάθειες όπου υπήρχαν στο Secure Sockets Layer. Η χρησιμότητα του συγκεκριμένου πρωτοκόλλου είναι για επικοινωνία μηχανής προς μηχανή. [14]

## *3.2 HTTP/HTTPS*

Το HTTP (Hypertext Transfer Protocol) όπως και το HTTPS το οποίο είναι το ασφαλές, είναι θεμελιώδη πρωτόκολλα επικοινωνίας. Επιτρέπουν την μεταφορά δεδομένων μεταξύ του χρήστη με χρήση ενός φυλλομετρητή και του αντίστοιχου προγράμματος ιστού. Κάθε αίτημα από έναν χρήστη προς τον διακομιστή είναι ανεξάρτητο και ο διακομιστής δεν διατηρεί τις πληροφορίες σχετικά με προηγούμενα αιτήματα. Τα αιτήματα και οι απαντήσεις βασίζονται σε κείμενο. Στο HTTP το κείμενο δεν είναι κρυπτογραφημένο.[14]

**Μέθοδοι αιτημάτων**

- Get → Ανάκτηση δεδομένων
- Post → Υποβολή δεδομένων
- Put → Ενημέρωση δεδομένων
- Delete → Διαγραφή δεδομένων
- Patch → Τροποποίηση Δεδομένων
- Head → Ανάκτηση κεφαλίδας δεδομένων
- Options → Ανάκτηση πληροφοριών
- Connect → Δημιουργία σύνδεσης
- Trace → Ιχνηλάτιση αλλαγών

**Κωδικοί κατάστασης**

Οι κωδικοί κατάστασης χωρίζονται σε κατηγορίες με βάση το εύρος

- 1** → Πληροφορία
- 2** → Επιτυχία
- 3** → Ανακατεύθυνση
- 4** → Σφάλμα πελάτη
- 5** → Σφάλμα διακομιστή

## *3.3 Bluetooth*

Η τεχνολογία Bluetooth ξεκίνησε στα τέλη της δεκαετίας του 1990 μέσω μιας συλλογικής προσπάθειας μεταξύ κορυφαίων εταιρειών τεχνολογίας. Σκοπός ήταν να απλοποιηθεί η ασύρματη επικοινωνία μικρής εμβέλειας. Με την άνοδο του Διαδικτύου των Πραγμάτων με εκατομμύρια ασύρματες συσκευές το Bluetooth αποτελεί βασικό πρωτόκολλο του Διαδικτύου των Πραγμάτων. Με την πάροδο του χρόνου, η τεχνολογία Bluetooth έχει εξελιχθεί σημαντικά, με διαδοχικές επαναλήψεις που εισάγουν βελτιώσεις στην ταχύτητα, την εμβέλεια και τις

δυνατότητες. Λόγω της ευκολίας που προσφέρει το Bluetooth στην σύνδεση συσκευών είναι πρωτόκολλο που υλοποιεί ο μεγαλύτερος αριθμός συσκευών.[27]

## *3.4 SSH*

Το SSH (Secure Shell) είναι ένα πρωτόκολλα κρυπτογραφίας δικτύου και επιτρέπει ασφαλή απομακρυσμένη πρόσβαση και επικοινωνία συσκευών. Η χρήση του στο Διαδίκτυο των Πραγμάτων δεν σχετίζεται με τις συσκευές του δικτύου αλλά με την κεντρική συσκευή ελέγχου του δικτύου. Το συγκεκριμένο πρωτόκολλο παρέχει ένα ασφαλές κανάλι για την εκτέλεση εντολών σε μια απομακρυσμένη συσκευή, στην περίπτωση του IOT η κύρια συσκευή έλεγχου είναι ένα raspberry pi. Μέσω του raspberry pi γίνετε ο έλεγχος των συσκευών, συλλογή δεδομένων, διαχείριση. Με την χρήση του SSH γίνονται ενημερώσεις λογισμικού και ενημερώσεις ασφάλειας. Μέσω του SSH γίνετε και μεταφορά δεδομένων υλοποιώντας ασφαλή πρωτόκολλα μεταφοράς δεδομένων όπως το SCP (Secure Copy Protocol) διασφαλίζοντας στον διαχειριστή ότι τα δεδομένα μεταφέρονται με ασφάλεια.[25]

## *3.5 Υλοποιήσεις Διαδικτύου των Πραγμάτων*

Το Διαδίκτυο των Πραγμάτων συμβάλει στην καθημερινότητα με μεγάλη ποικιλία από υλοποιήσεις. Το εύρος καλύπτει απλές υλοποιήσεις οι οποίες συναντάμε σε κάποιο έξυπνο σπίτι, περίπλοκες λύσεις μεγαλύτερου εύρους όπως συγκεκριμένες ενέργειες σε μια πόλη ή ακόμα μεγαλύτερης κλίμακας οπού αφορούν θέματα υγείας και ολοκληρωμένες λύσεις σε μια έξυπνη πόλη.[6]

**Μικρής κλίμακας**

- Έξυπνο σπίτι: έλεγχος φωτισμού, θερμοστάτη, πόρτα, χρήση οικιακών συσκευών, απομακρυσμένος έλεγχος.
- Ασφάλεια: έλεγχος περιοχής με χρήση κάμερας, έλεγχος της κάμερας.
- Οικιακές συσκευές: Έξυπνο ρολόι, καφετιέρα.

**Μεσαίας κλίμακας**

- Ενέργειες Έξυπνης πόλης: φωτισμός δρόμου, ποιότητα αέρα, πάρκινγκ.

**Ολοκληρωμένες ενέργειες λύσης**

- Διαχείριση σηματοδοτών κυκλοφορίας.
- Διαχείριση κυκλοφορίας.
- Σενάριο καταστροφής.
- Βέλτιστη απόκριση υπηρεσιών υγείας.
- Βέλτιστη απόκριση υπηρεσιών νόμου.

Οι Υλοποιήσεις που αναφέρθηκαν είναι ευάλωτες σε επιθέσεις. Η αναλογία κλίμακας με τεχνογνωσία επίθεσης δεν ισχύει. Απλές επιθέσεις οι οποίες είναι ενεργές για μικρή κλίμακα είναι το ίδιο αποτελεσματικές σε Ολοκληρωμένες ενέργειες λύσης. Αυτό είναι ένα κρίσιμο σημείο στην εξάπλωση του Διαδικτύου των Πραγμάτων διότι πετυχημένες επιθέσεις μεγάλης κλίμακας θέτουν σε κίνδυνο την ακεραιτότητα του χρήστη.

# 4 ΑΠΕΙΛΕΣ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

## *4.1 Ομάδες Ransomware*

Τα τελευταία χρόνια, η άνοδος των εξελιγμένων ομάδων ransomware έχει αποτελέσει σημαντική απειλή για την ασφάλεια στον κυβερνοχώρο παγκοσμίως. Οι ομάδες Ransomware χρησιμοποιούν προηγμένες τεχνικές για να παραβιάσουν συστήματα ώστε να κρυπτογραφούν δεδομένα και να εκβιάζουν τους κατόχους με οικονομικό αντίκτυπο. Οι ομάδες ransomware είναι οργανωμένες εγκληματικές ομάδες στον χώρο της κυβερνοασφάλειας με σκοπό την ανάπτυξη κακόβουλου λογισμικού για την κρυπτογράφηση των δεδομένων των θυμάτων τους. Εκτός από το οικονομικό αντίκτυπο οι επιθέσεις από ομάδες ransomware κάνουν ζημιά στην φήμη ενός οργανισμού. Οι έξυπνες πόλεις θα αποτελέσουν μεγάλο στόχο αυτόν των ομάδων. Τομείς υποδομής ζωτικής σημασίας, ιδρύματα υγειονομικής περίθαλψης, ακόμη και κυβερνητικές υπηρεσίες έχουν πέσει θύματα ransomware. Οι ομάδες ransomware έχουν κυρίως οικονομικά κίνητρα, αναζητώντας σημαντικές πληρωμές σε κρυπτονομίσματα από τα θύματά τους. Η ανωνυμία που παρέχεται από τις συναλλαγές με κρυπτονομίσματα καθιστά δύσκολο τον εντοπισμό και τη σύλληψη αυτών των εγκληματιών στον κυβερνοχώρο. Μπροστά στις απειλές που δημιουργούν οι ομάδες ransomware ένα Κέντρο Ασφαλείας δρα ως βασικός άξονας στην αμυντική στάση ενός οργανισμού.[1] [28]

## *4.2 Εκμετάλλευση συσκευών*

Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί τρωτά σημεία σε συσκευές του Διαδικτύου των Πραγμάτων ώστε να αποκτήσει πρόσβαση και έλεγχο. Οι συσκευές οι οποίες έχουν παραβιαστεί μπορούν να χρησιμοποιηθούν από τον επιτιθέμενο προς δικό του όφελος, να υπολειτουργούν ή να τεθούν εκτός λειτουργίας με σκοπό μία επίθεση άρνησης λειτουργίας. Με ένα Επιχειρησιακό Κέντρο Ασφαλείας μπορούμε να προλάβουμε την ζημιά μίας τέτοιας επίθεσης μέσω ανάλυσης της συμπεριφοράς μίας συσκευής. Οι αναλυτές θα εντοπίσουν το περιστατικό και θα απομονώσουν την παραβιασμένη συσκευή ώστε να ελαχιστοποιηθεί η ζημιά. Με τακτικές ενημερώσεις και αξιολογήσεις ευπαθειών προλαμβάνουμε επιθέσεις ώστε να υπάρχει μεγαλύτερη ασφάλεια στο σύστημα μας.[24]

### *4.3 Άρνηση υπηρεσίας*

Οι επιτιθέμενοι μπορούν να πλημμυρίσουν το δίκτυο μίας έξυπνης πόλης προκαλώντας διακοπές στην παροχή υπηρεσίας. Το Κέντρο Ασφαλείας μετριάζει την επίθεση με συστήματα ανίχνευσης εισβολής εντοπίζοντας ασυνήθιστα μοτίβα στο δίκτυο. Μπορούμε να δημιουργήσουμε φίλτρο στην κυκλοφορία ώστε να αποκλείσουμε τους επιτιθέμενους. [13]

### *4.4 Υποκλοπές δεδομένων*

Τα δεδομένα τα οποία ανταλλάσσονται μεταξύ των συσκευών του Διαδικτύου των Πραγμάτων στα πλαίσια μίας έξυπνης πόλης μπορούν να υποκλαπούν και να χειραγωγηθούν από έναν επιτιθέμενο. Η υποκλοπή δεδομένων ενδέχεται να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες των κατοίκων της πόλης. Με την υλοποίηση ενός Κέντρου Ασφαλείας έχουμε πρωτόκολλα κρυπτογράφησης και ασφαλή κανάλια επικοινωνίας ώστε να προστατευτούν τα δεδομένα κατά την μεταφορά όπως και ασφαλή αποθήκευση δεδομένων. Το Κέντρο Ασφαλείας επίσης παρακολουθεί την κυκλοφορία του δικτύου ώστε να εντοπίσει την επίθεση και να αποτρέψει μία μη εξουσιοδοτημένη πρόσβαση. [24]

### *4.5 Εσωτερική απειλή*

Διαχειριστές και εργατικό δυναμικό της πόλης με κακόβουλη πρόθεση ενδέχεται να κάνουν κατάχρηση της πρόσβασης τους για να παραβιάσουν συσκευές, δεδομένα ή συστήματα της έξυπνης πόλης. Έχοντας ένα λειτουργικό Κέντρο Ασφαλείας αναλύουμε τα στοιχεία συμπεριφοράς των χρηστών και εντοπίζουμε ανωμαλίες ενεργειών από κατόχους πληροφοριών. [24]

### *4.6 Παραβάσεις απορρήτου*

Η συλλογή και η χρήση προσωπικών δεδομένων των συσκευών οδηγεί σε παραβίαση προσωπικού απορρήτου. Τα μέτρα προστασίας δεδομένων με κρυπτογραφία όπως και η μετατροπή των δεδομένων σε ανώνυμα δεδομένα παρέχουν προστασία σε παραβάσεις απορρήτου.[24]

### *4.7 Φυσικές παραβιάσεις*

Φυσικές επιθέσεις όπως μία παραβίαση κάποιου αισθητήρα ή μίας κάμερας, απενεργοποίηση της συσκευής θέτουν σε κίνδυνο τα δεδομένα τα οποία διατηρεί μία έξυπνη πόλη. Φυσικές φθορές όπως και απώλεια εξοπλισμού ή δεδομένων μέσα από κλοπή εξοπλισμού αποθήκευσης δεδομένων είναι μέσα στις απειλές τις οποίες βρίσκετε απέναντι μία έξυπνη πόλη. Το Κέντρο Ασφαλείας είναι υπεύθυνο ώστε να ορίσει τα μέτρα φυσικής ασφαλείας, μαζί με τους ελέγχους οι οποίοι θα γίνονται για την πρόσβαση στον εξοπλισμό. Οι φυσικές παραβιάσεις εντοπίζονται με την διαδικασία παρακολούθησης με την βοήθεια των αναλυτών.[24]

### *4.8 Shodan*

Το Shodan είναι μια μηχανή αναζήτησης του διαδικτύου. Σε αντίθεση με γνωστές μηχανές αναζήτησης που παρέχονται από την Google και Microsoft, το Shodan εξειδικεύεται στο να εντοπίζει συσκευές, διακομιστές και ολοκληρωμένα συστήματα. Παρέχει πληροφορίες σχετικά των ευάλωτων σημείων και ταξινομεί τα αποτελέσματα με βάση το αποτύπωμα που αφήνει η κάθε διεύθυνση. Αποτελεί σημαντικό εργαλείο ερευνητών ασφάλειας, αλλά γίνετε παράνομη χρήση και από κακόβουλους χρήστες[16]. Ο τρόπος λειτουργίας του Shodan είναι ο εξής:

- Σαρώνει το διαδίκτυο για συσκευές.
- Σαρώνει τις υπηρεσίες που υλοποιούν.
- Αναγνωρίζει ευάλωτες υπηρεσίες.
- Παρακολουθεί τις συσκευές.

- Παρέχει φίλτρα για την αναζήτηση.

Με βάση τα φίλτρα που παρέχει το Shodan οι χρήστες μπορούν να αναζητήσουν συγκεκριμένου τύπου συσκευές όπως κάμερες ασφαλείας με εργοστασιακούς κωδικούς πρόσβασης. Η σωστή χρήση φίλτρων είναι ιδιαίτερα επικίνδυνη προς το Διαδίκτυο των Πραγμάτων. Οι χρήστες μπορούν να εμφανίσουν αποτελέσματα με βάση:

- Τοποθεσία / Πόλη / Χώρα :
- Hostname
- Port : 22, 23 (ssh, ftp)
- Λειτουργικό Σύστημα : rasbian, android
- Όνομα συσκευής
- Εκτελέσιμη υπηρεσία : apache
- Ευπάθειες: CVE-xxxx-xxxx
- Έκδοση
- Τύπο συσκευής: κάμερα, δρομολογητής, τηλεόραση.

Το Shodan είναι ένα ισχυρό εργαλείο για επαγγελματίες ασφάλειας, αλλά παραμένει απειλή για το Διαδίκτυο των Πραγμάτων. Οτιδήποτε είναι συνδεμένο στο διαδίκτυο μόνιμα και εκπέμπει, είναι θέμα χρόνου να εμφανιστεί στην βάση δεδομένων του Shodan.[22]

## *4.9 Απομακρυσμένες Επιθέσεις*

Με την χρήση του Shodan κακόβουλοι χρήστες μπορούν να εντοπίσουν ευάλωτες συσκευές και με τα εργαλεία του Kali Linux να εκτελέσουν επιθέσεις[16][7].

- Απομακρυσμένη εκτέλεση κώδικα
- Αυθεντικοποίηση σε σελίδα εισόδου
- Επιθέσεις μη-αναβαθμισμένου λογισμικού
- Άρνησης υπηρεσίας

- Δημιουργία Botnet
- Επιθέσεις σε ευάλωτα πρωτόκολλα
- Υποκλοπές

### *4.10 Επιθέσεις Μικρής Απόστασης*

Αντίθετα με τις απομακρυσμένες επιθέσεις που μπορούν να εκτελεστούν από οποιοδήποτε σημείο στον κόσμο. Στις επιθέσεις μικρής απόστασης ο στόχος και ο επιτιθέμενος είναι σε κοντινή απόσταση. Βασίζονται σε ασύρματες τεχνολογίες και σε πρωτόκολλα που υλοποιούν οι συσκευές στο διαδίκτυο των πραγμάτων.[24][4]

- Bluetooth
- IEEE 802.11
- Man in the Middle
- RFID
- NFC
- Jamming
- Dos

Ανάλογα την απόσταση και την πρόσβαση που έχει ο επιτιθέμενος υπάρχει και η δυνατότητα επίθεσης στο υλικό της συσκευής. Αν υπάρχει φυσική πρόσβαση το κλείσιμο της συσκευής κατατάσσεται σε επίθεση άρνησης υπηρεσίας.

# 5 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΗΣ

Συστήματα ανίχνευσής εισβολής είναι οι τεχνολογίες ασφάλειας που παρακολουθούν το δίκτυο ή δραστηριότητα στο σύστημα για οποιοδήποτε μορφή ανωμαλίας ή κακόβουλη χρήση. Τα συστήματα ανίχνευσης εισβολής κατατάσσονται σε δύο βασικές κατηγορίες. Συστήματα που βασίζονται στο δίκτυο και συστήματα που βασίζονται σε έναν κεντρικό υπολογιστή.[5]

- Συστήματα ανίχνευσής εισβολής δικτύου: Παρακολουθούν το δίκτυο αναλύοντας πακέτα δεδομένων ώστε να γίνει ανίχνευση από ανωμαλίες στο δίκτυο ή υπογραφές που αφήνουν γνωστές επιθέσεις. Με τον εντοπισμό ύποπτης δραστηριότητας ειδοποιεί τον χρήστη ή το προσωπικό ασφάλειας ώστε να γίνει διερεύνησης.

- Συστήματα ανίχνευσής εισβολής κεντρικού υπολογιστή: Το σύστημα ανίχνευσης εισβολής εγκαθίσταται στον κεντρικό υπολογιστή ή σε συσκευές του δικτύου και παρακολουθεί τοπικές δραστηριότητες. Αρχεία, αλλαγές σε αρχεία καταγραφής, ανωμαλίες στην πρόσβαση, σημάδια κακόβουλου λογισμικού στο επίπεδο της συσκευής που έχει γίνει η εγκατάσταση.

## *5.1 Αναγκαιότητα συστημάτων*

Τα συστήματα ανίχνευσης εισβολών κατέχουν κεντρικό ρόλο στην κυβερνοασφάλεια. Η άνοδος του διαδικτύου των πραγμάτων τα καθιστά απαραίτητα. Έχουν σχεδιαστεί ώστε να είναι φρουροί και να παρακολουθούν συνεχώς την κυκλοφορία του δικτύου σε πραγματικό χρόνο. Παρέχουν στους οργανισμούς και τους χρήστες την δυνατότητα να εντοπίζουν και να μπορούν να ανταποκριθούν άμεσα σε περιστατικά ασφάλειας. Σε όλα τα περιστατικά ασφάλειας ο χρόνος απόκρισης έχει κρίσιμο ρόλο. Βασικό χαρακτηριστικό είναι η ελαχιστοποίηση του χρόνου, ειδοποιώντας τους χρήστες για τις παραβιάσεις.[32]

## *5.2 Τρόπος λειτουργίας*

Βασικά χαρακτηριστικά στην λειτουργία ενός συστήματος ανίχνευσης εισβολής τα οποία υλοποιούν και οι δύο κατηγορίες:

- **Ανίχνευση με βάση υπογραφής**: Υπάρχουν προκαθορισμένες υπογραφές και συμπεριφορές γνωστών επιθέσεων. Η συγκεκριμένη μέθοδος είναι αποτελεσματική για αναγνώριση κακόβουλου λογισμικού και γνωστών επιθέσεων αλλά δεν προσφέρει ασφάλεια σε καινούριες επιθέσεις όπως zero day attacks.
- **Ανίχνευση με βάση ανωμαλίας**: Ορίζοντας μια κανονική συμπεριφορά του δικτύου ή του συστήματος, θεωρούμε πως οποιαδήποτε απόκλιση από την ροή που έχουμε ορίσει είναι κακόβουλη επίθεση. Η συγκεκριμένη μέθοδος είναι αποτελεσματική για επιθέσεις zero day αλλά δημιουργεί και ψευδώς θετικά αποτελέσματα τα οποία στην συνέχεια μετατρέπονται σε ειδοποιήσεις.
- **Ειδοποίηση**: Το σύστημα δημιουργεί ειδοποιήσεις για κάθε ύποπτη δραστηριότητα την οποία εντοπίζει. Οι ειδοποιήσεις αυτές στέλνονται στον χρήστη ή το προσωπικό ασφάλειας. Οι ειδοποιήσεις καταγράφονται ώστε να γίνει χρήση στο μέλλον για ανάλυση ή ενσωμάτωση σε άλλα εργαλεία ώστε να γίνει αυτοματοποιημένα η ανάλυση.
- **Παρακολούθηση**: Το σύστημα παρακολουθεί συνεχώς την δραστηριότητα του δικτύου ή του κεντρικού υπολογιστή συλλέγοντας δεδομένα.

Το σύστημα ανίχνευση εισβολής της επιλογής μας είναι το Snort.

## *5.3 Snort*

Το Snort είναι ένα σύστημα ανίχνευσης εισβολής ανοιχτού κώδικα (IDS) που παίζει καθοριστικό ρόλο στην ασφάλεια του δικτύου. Ως λογισμικό ανοιχτού κώδικα το Snort επωφελείται από μια μεγάλη κοινότητα προγραμματιστών και χρηστών που συμβάλλουν συνεχώς στη βελτίωση και την ανάπτυξή του όπως και το Linux. Αυτό το πλεονέκτημα ενισχύει την καινοτομία και διασφαλίζει ότι το Snort παραμένει ενημερωμένο και στην πρώτη γραμμή της άμυνας του δικτύου. Με τη συνεχή παρακολούθηση της κυκλοφορίας του δικτύου και των δραστηριοτήτων του

συστήματος δίνετε η δυνατότητα εντοπισμού κακόβουλης συμπεριφοράς άμεσα ώστε να υπάρχει ανταπόκριση σε πιθανές απειλές. Είναι ευέλικτο λογισμικό και κατάλληλο για μεγάλο φάσμα από μικρά πρότζεκτ μέχρι μεγάλες επιχειρήσεις. Μπορεί να προσαρμοστεί ώστε να ευθυγραμμίζεται με τις συγκεκριμένες ανάγκες ασφαλείας ανά περίσταση. Το Snort εξουσιοδοτεί τις ομάδες ασφαλείας με έγκαιρες ειδοποιήσεις και ειδοποιήσεις, παρέχοντας βασικές πληροφορίες για έρευνες και αντιμετώπιση περιστατικών. Η απρόσκοπτη ενσωμάτωσή του σε ευρύτερες αρχιτεκτονικές ασφαλείας το καθιστά αναπόσπαστο συστατικό των ολοκληρωμένων αμυντικών στρατηγικών.[18]

# 6 ΠΕΙΡΑΜΑ

## *6.1 ΟΜΑΔΕΣ*

Στον χώρο της κυβερνοασφάλειας κυριαρχούν 2 ομάδες, η μπλε και η κόκκινη. Η μπλε ομάδα είναι υπεύθυνη για την ασφάλεια των συστημάτων και αντιπροσωπεύει την αμυντική πλευρά. Εφαρμόζουν μέτρα ασφαλείας, αξιολογούν τον κίνδυνο, παρακολουθούν την κυκλοφορία του δικτύου και αναλύουν τα περιστατικά προς αντιμετώπιση. Η κόκκινη ομάδα αντιπροσωπεύει την επιθετική πλευρά, προσομοιώνει επιθέσεις στα συστήματα ενός οργανισμού ώστε να βρει τρωτά σημεία και αδυναμίες. Στόχος είναι να αποκαλυφθούν ελαττώματα ασφαλείας που μπορεί να μην είναι εμφανή στην μπλε ομάδα του οργανισμού ώστε να παρέχει συστάσεις για βελτίωση. Οι ομάδες συνεργάζονται και έχουν κοινό σκοπό να βελτιστοποιηθεί η ασφάλεια του οργανισμού. Σημαντικός ρόλος της κόκκινης ομάδας είναι να κάνει την μπλε ομάδα καλύτερη, διότι η μπλε ομάδα είναι υπεύθυνη για την ασφάλεια του οργανισμού. Στο πείραμα η μπλε ομάδα είναι υπεύθυνη για την δημιουργία των κανόνων και η κόκκινη ομάδα για την προσομοίωση της επίθεσης σάρωσης.

## *6.2 RASPBERRY PI*

Το Raspberry Pi είναι ένας μικρός αλλά ικανός υπολογιστής μονής πλακέτας. Έχει αναδειχθεί στον κόσμο της τεχνολογίας από την έναρξη του το 2012 και αυξάνει τις δυνατότητες του με την ανάπτυξή του Διαδικτύου των Πραγμάτων. Είναι σχεδιασμένο και αναπτύσσετε από το ίδρυμα Raspberry Pi και το λογισμικό που χρησιμοποιεί είναι το raspbian το οποίο είναι μία Debian based Linux διανομή. Το μικρό μέγεθος του το καθιστά ένα ευέλικτο και οικονομικά αποδοτικό εργαλείο για πολλές εφαρμογές.[15] Στο πλαίσιο του Διαδικτύου των Πραγμάτων το Raspberry Pi έχει κρίσιμο ρόλο για τους ακόλουθους λόγους:

- Τιμή
- Ευελιξία
- Συνδεσιμότητα
- GPIO Pins
- Κοινότητα

- Εκπαίδευση
- Υλοποίηση πρότζεκτ IoT

## *6.3 Raspbian*

Το Raspbian είναι το λειτουργικό σύστημα που σχεδιάστηκε ειδικά για το Raspberry Pi. Το Raspbian είναι το προεπιλεγμένο και προτεινόμενο λειτουργικό σύστημα για όλα τα μοντέλα Raspberry Pi. Είναι χτισμένο στα γερά θεμέλια του λειτουργικού συστήματος Debian και έχει βελτιστοποιηθεί για να προσφέρει μια εξαιρετική εμπειρία υπολογιστών προσαρμοσμένη στις δυνατότητες του υλικού Raspberry Pi. Οι πρωταρχικοί στόχοι του Raspbian είναι να παρέχει ένα φιλικό προς τον χρήστη, ευέλικτο και αποτελεσματικό περιβάλλον υπολογιστών για τους χρήστες του Raspberry Pi, ιδιαίτερα στους τομείς της εκπαίδευσης, του πειραματισμού και της ανάπτυξης IoT. Τα βασικά χαρακτηριστικά του Raspbian περιλαμβάνουν ένα φιλικό προς το χρήστη γραφικό περιβάλλον επιφάνειας εργασίας και εγκατεστημένα πακέτα λογισμικού. Το Raspbian χρησιμεύει ως το θεμέλιο πάνω στο οποίο χτίζονται αμέτρητα καινοτόμα έργα και μαθησιακές εμπειρίες.

## *6.4 Kali Linux*

Το Kali Linux είναι ένα λογισμικό που έχει σχεδιαστεί και χρησιμοποιείται για δοκιμές ασφάλειας. Παρέχει μεγάλο αριθμό εργαλείων για δοκιμές ασφάλειας όπως για κρυπτογραφία και μεθοδολογίες ιατροδικαστικής δεδομένων. Είναι λογισμικό ανοιχτού κώδικα. Μπορεί να εκτελεστεί με χρήση εικονικής μηχανής κάτι που το κάνει προσβάσιμο από χρήστες που δεν έχουν εξοικείωση με διανομές Linux. [11]Ο λόγος που χαρακτηρίζετε απειλή είναι πως τα εργαλεία που διαθέτει για δοκιμές διείσδυσης από επαγγελματίες ασφάλειας είναι τα ίδια εργαλεία που χρησιμοποιούν κακόβουλοι χρήστες.

## *6.5 Nmap*

Το Nmap είναι ένα ισχυρό εργαλείο σάρωσης δικτύου ανοιχτού κώδικα που χρησιμοποιείται για την για έλεγχο ασφάλειας στο δίκτυο. Είναι λογισμικό ανοιχτού κώδικα και αναπτύχθηκε και αναβαθμίζετε από μία κοινότητα επαγγελματιών ασφάλειας. Κύρια λειτουργία του είναι να χαρτογραφεί δίκτυα, να αναγνωρίζει κεντρικούς υπολογιστές και να συλλέγει βασικές πληροφορίες σχετικά με τις υπηρεσίες και τις διαμορφώσεις του δικτύου. Υλοποιεί Script τα οποία έχουν δημιουργηθεί από την κοινότητα ώστε να δίνει πληροφορίες για το λογισμικό και τις υπηρεσίες οι οποίες υλοποιούνται στους στόχους του[23].

- Ανακάλυψη δικτύου
- Σάρωση θυρών
- Αναγνώριση υπηρεσίας
- Αναγνώριση λειτουργικού συστήματος
- Αναγνώριση CVE

**Δημιουργεί λεπτομερείς αναφορές οι οποίες αποθηκεύονται για μελλοντική χρήση κάτι που το καθιστά κατάλληλο εργαλείο για δοκιμές ασφάλειας. Είναι ένα απαραίτητο εργαλείο για επαγγελματίες ασφάλειας όπως και για δοκιμές διείσδυσης.**

## *6.6 Nmap ίδια διεύθυνση IP*

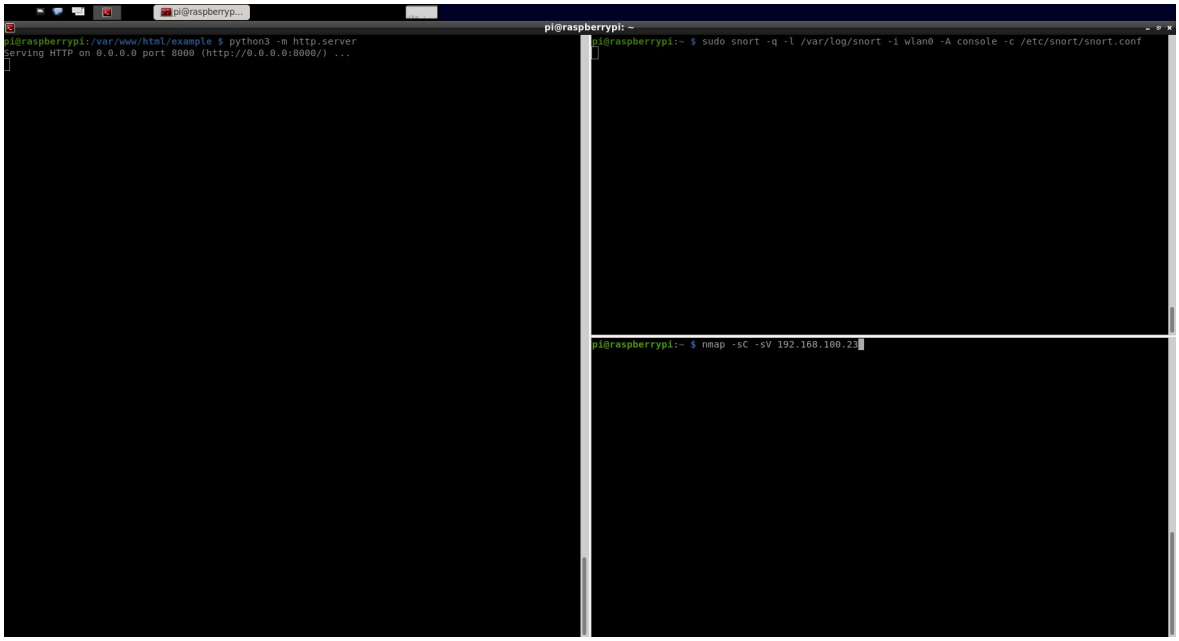
Αφού έχει γίνει εγκατάσταση του Raspbian και του Snort στο Raspberry Pi μπορούμε να ξεκινήσουμε την εκτέλεση του πειράματος ώστε να υλοποιηθεί ένα Κέντρο ασφάλειας.

1. Ενεργοποιούμε έναν απλό http server.
2. Ενεργοποιούμε το snort.
3. Εκτελούμε το nmap από το raspberry pi.

```
1 python3 -m http.server
```

```
1 sudo snort -q -l /var/log/snort -i <interface> -A console -c /etc/snort/snort.conf
```

```
1 nmap -sC -sV 192.168.100.23
```

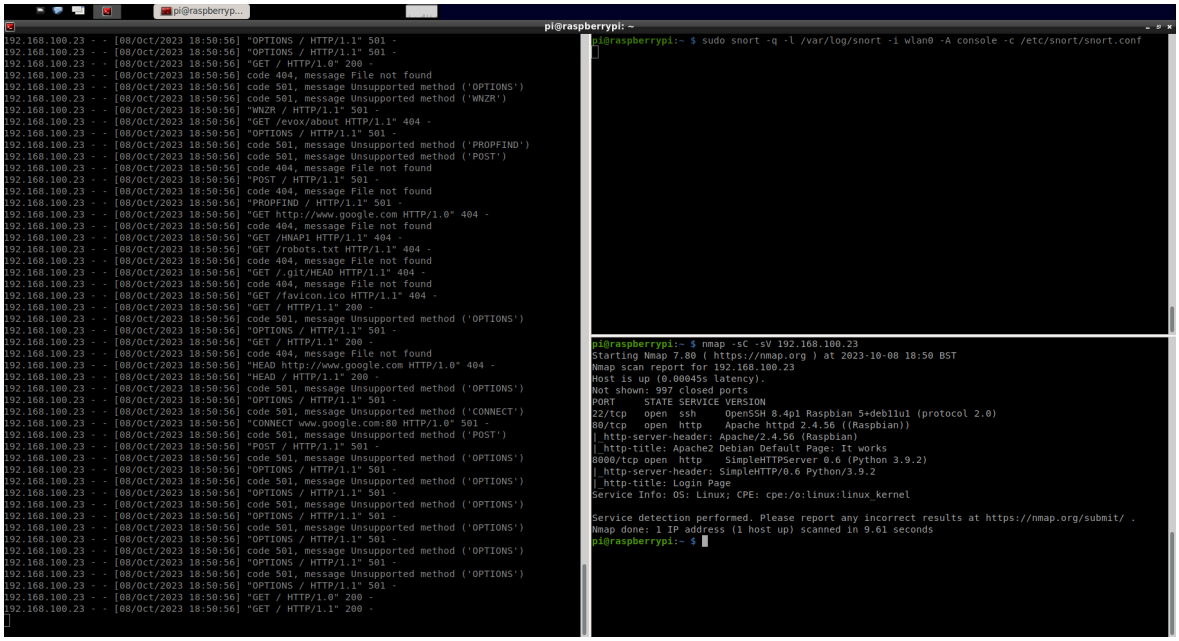



*Σχήμα 1: Δοκιμή ίδιας διεύθυνσης IP*

Όπως βλέπουμε στα αποτελέσματα το τερματικό του server δείχνει τα αιτήματα που έχουν σταλεί από το nmap αλλά το σύστημα εντοπισμού εισβολής παραμένει κενό. Με βάση τους κανόνες που έχουμε ορίσει το snort δεν δημιουργεί αναφορές για ανωμαλίες στο δίκτυο και απειλές οι οποίες προέρχονται από την ίδια διεύθυνση οπού υλοποιείτε το σύστημα ανίχνευσής. Σκοπός είναι να αποφύγουμε ψευδώς αληθές αναφορές δεδομένου πως ο επιτιθέμενος δεν μπορεί να είναι ο ίδιος ο αμυνόμενος.

Στο τερματικό του nmap μπορούμε να δούμε αναλυτικά τα αποτελέσματα από τις υπηρεσίες τις οποίες υλοποιεί το raspberry pi

- ssh port 22
- http port 80
- http port 8000



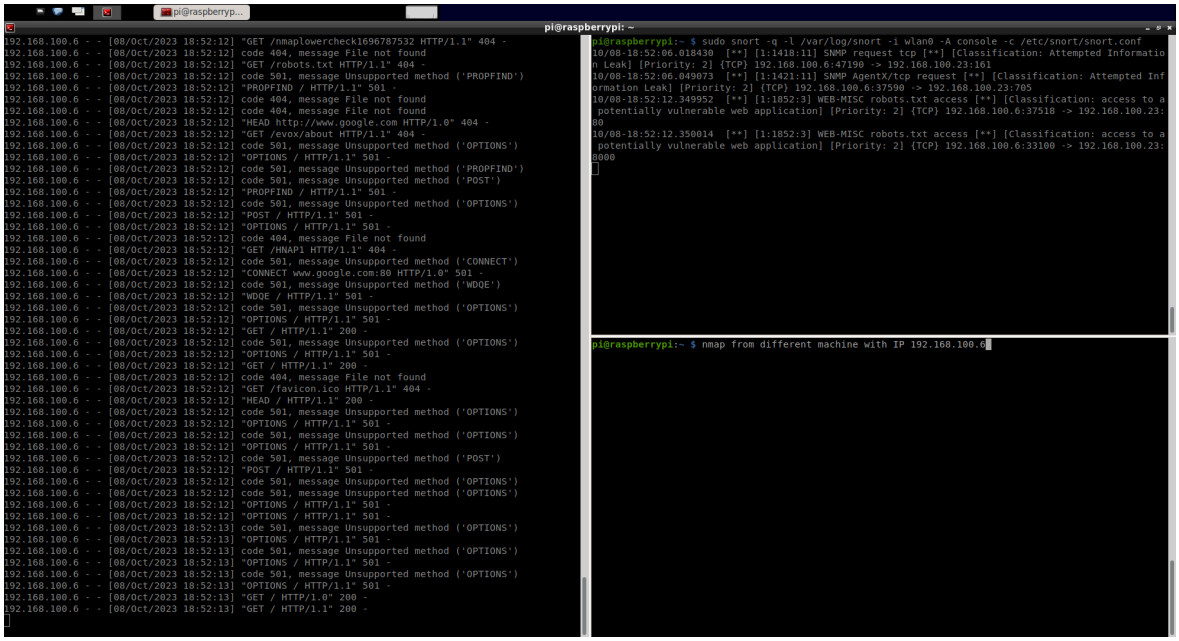

*Σχήμα 2: Δοκιμή ίδιας διεύθυνσης IP 2*

## *6.7 Nmap διαφορετική IP*

Όταν γίνετε εκτέλεση του nmap από διαφορετική IP από αυτή που έχουμε ορίσει ως HOME μπορούμε να δούμε πως το snort δημιουργεί αναφορά για το συμβάν. Οι δομή της αναφοράς:

- Ημερομηνία / Χρόνος
- Μήνυμα
- Προτεραιότητα
- Ταξινόμηση
- Διεύθυνση επιτιθέμενου
- Θύρα υλοποίησης επιτιθέμενου

- Διεύθυνση θύματος
- Θύρα υλοποίησης θύματος
- Πρωτόκολλο
- Εμπλουτισμένα δεδομένα




*Σχήμα 3: Δοκιμή διαφορετικής διεύθυνσης IP*

Όπως βλέπουμε με τους απλούς κανόνες είναι δυνατό να εντοπιστεί η απειλή αναλυτικά και να ενημερωθούμε για τον τύπο της επίθεσης μέσω της αυτόματης ταξινόμησης όπου κατατάσσει το nmap σε επίθεση διαρροής πληροφοριών.[2]

## *6.8 Εμπλουτισμένες αναφορές*

Όπως αναφέραμε μπορούμε να φτιάξουμε δικούς μας κανόνες για το snort. Δημιουργώντας το αρχείο demonstration.rules στον φάκελο /etc/snort/rules οπού είναι ορισμένος φάκελος της μεταβλητής **RULE_PATH** μπορούμε να δημιουργήσουμε τους κανόνες. Πρέπει να γίνει αναβάθμιση στο κεντρικό αρχείο του snort /etc/snort/snort.config. [3][26]

```
sudo  touch /etc/snort/rules/demonstration.rules
sudo vim /etc/snort/rules/demonstration.rules
```

προσθέτουμε τους κανόνες

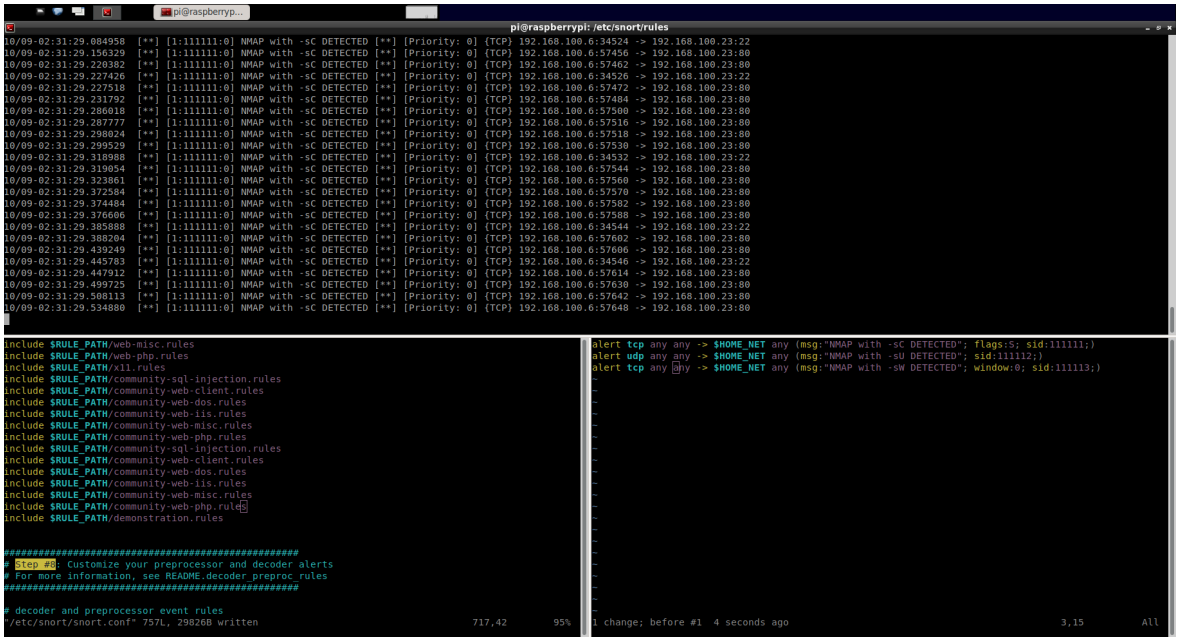
```
alert tcp any any → $HOME_NET any (msg"NMAP with -sC DETECTED"; flags:5; sid:1111111;)
alert tcp any any → $HOME_NET any (msg"NMAP with -sU DETECTED"; sid:1111112;)
alert tcp any any → $HOME_NET any (msg"NMAP with -sw DETECTED"; window:0; sid:1111113;)
```

```
sudo vim /etc/snort/snort.config
```

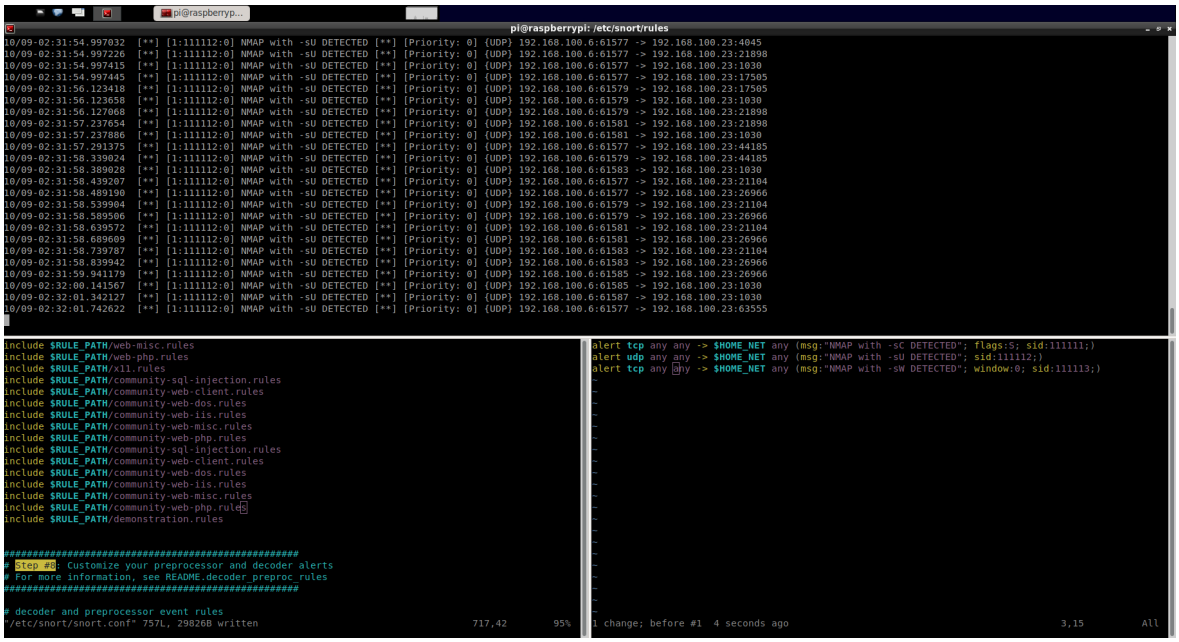
προσθέτουμε το αρχείο

```
include $RULE_PATH/demonstration.rules
```

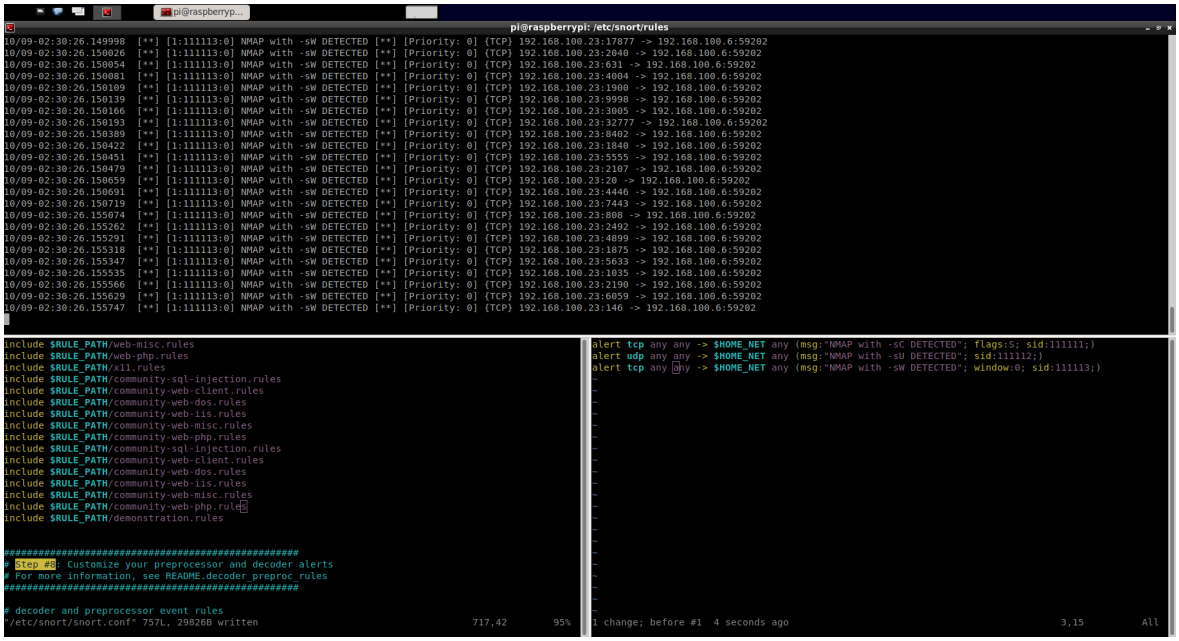
Στην έναρξη της επίθεσης τα αποτελέσματα είναι τα εξής




*Σχήμα 4: nmap enrichment -sC*




*Σχήμα 5: nmap enrichment -sU*




*Σχήμα 6: nmap enrichment -sW*

Βλέπουμε πως με βάση τους καινούριους κανόνες το μήνυμα στην αναφορά έχει αλλάξει και αναγνωρίζει το εργαλείο αλλά και την παράμετρο την οποία χρησιμοποιήθηκε για την εκτέλεση της επίθεσης. Παρόμοιοι κανόνες μπορούν να εφαρμοστούν για:

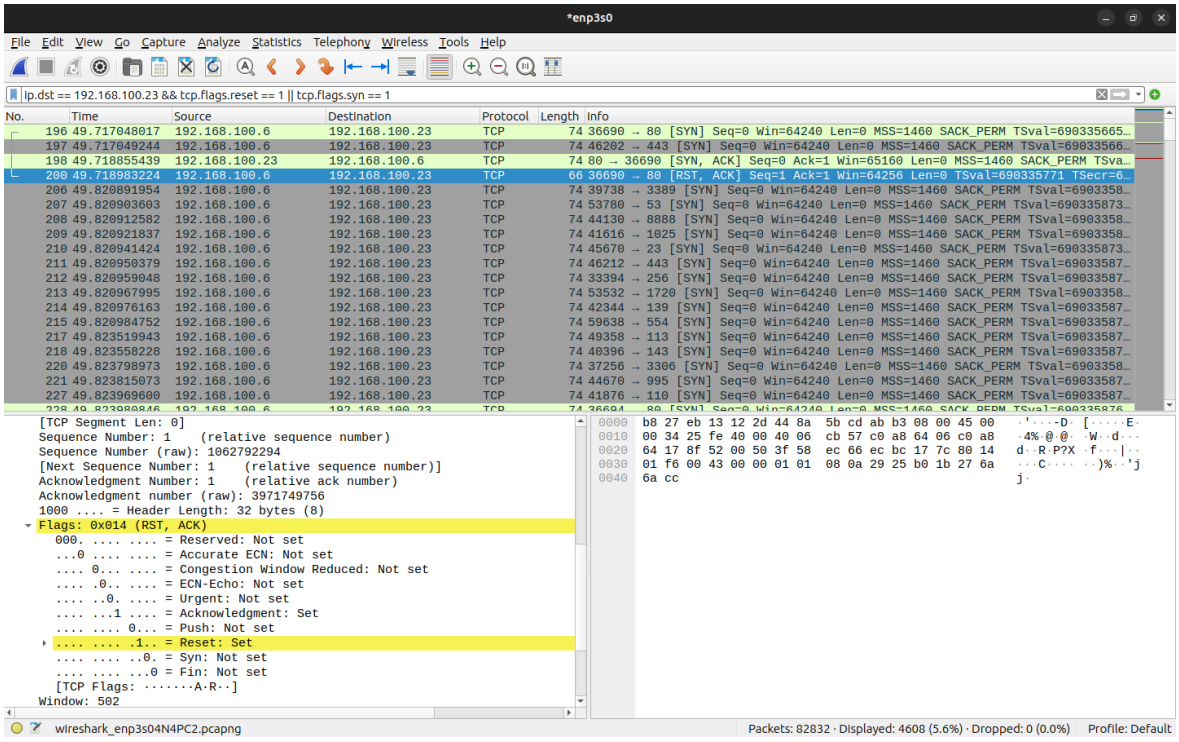
- Brute force
- ssh logins
- Web crawlers

## *6.9 Δημιουργία κανόνων με χρήση Wireshark*

Το wireshark είναι ένα εργαλείο ανάλυσης δικτύου ανοιχτού κώδικα. Με το wireshark μπορούμε να αναλύσουμε την κυκλοφορία και τις επικοινωνίες του δικτύου σε πραγματικό χρόνο.[19] Μια επιπλέον επιλογή του wireshark είναι να αναλύουμε δεδομένα τα οποία έχουν αποθηκευτεί σε κατάλληλη μορφή. Χαρακτηριστικά λειτουργίας του wireshark:[30]

- Συλλογή πακέτων
- Ανάλυση πακέτων
- Αποκωδικοποίηση πακέτων
- Χρήση φίλτρων
- Επιθεώρηση πακέτων
- Ανάλυση πρωτοκόλλου
- Ανάλυση ροής
- Εξαγωγή δεδομένων

Έχοντας ανοιχτό το wireshark ξεκινάμε την συλλογή πακέτων ώστε να αναλύσουμε την ροή στο δίκτυο για να μπορέσουμε να φτιάξουμε τους κανόνες για το snort. Εκτελούμε το nmap και αναλύουμε τα αποτελέσματα.




*Σχήμα 7: Ανάλυση nmap -sC*

Διαβάζοντας το manual του nmap βλέπουμε πως η συγκεκριμένη παράμετρος χρησιμοποιεί την κατηγορία default script . Στην σελίδα του nmap μπορούμε να δούμε τις κατηγορίες ώστε να δημιουργήσουμε τον κανόνα ανάλογα.

- Auth
- Broadcast
- Brute
- Default
- Discovery
- Dos
- Exploit
- External
- Fuzzer
- Intrusive
- Malware
- Safe
- Version
- Vuln

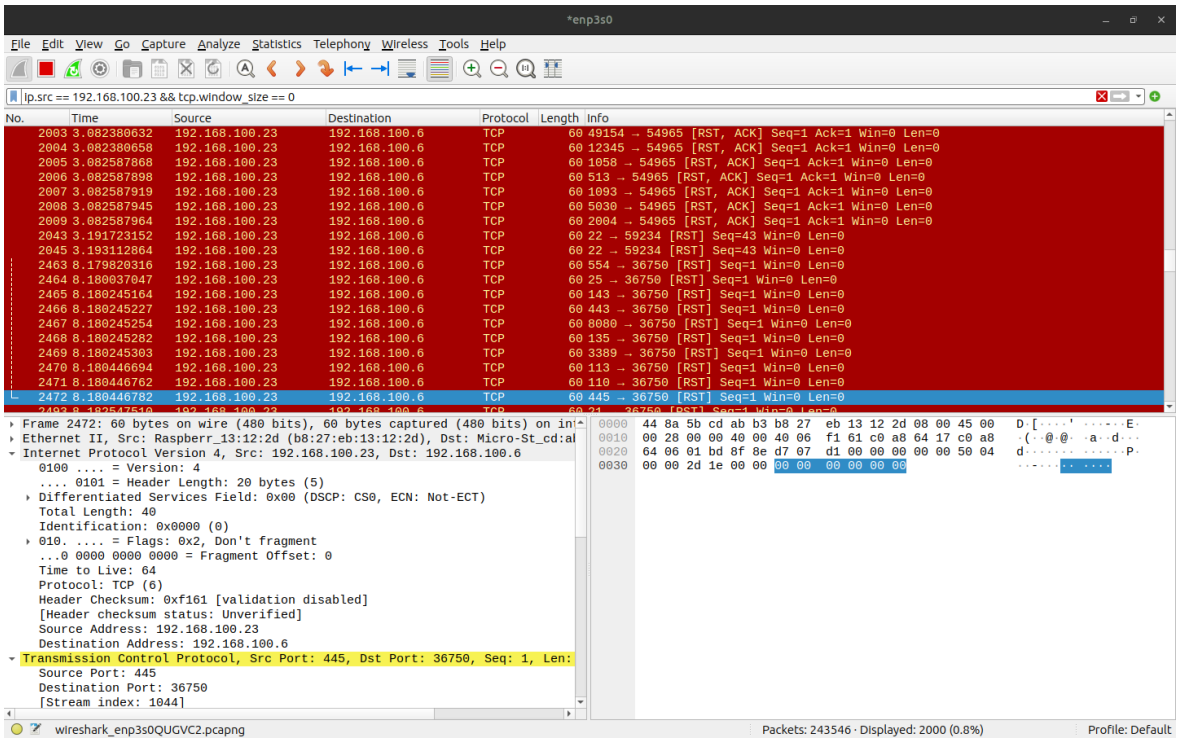
Τα αποτελέσματα από το Σχήμα 7: ανάλυση nmap -sC έχουν φίλτρο

- ip.dst = IP του θύματος
- tcp.flags.reset == 1 ώστε να είναι ενεργό το flag reset
- tcp.flags.syn == 1 ώστε να είναι ενεργό το flag syn

Μέσω την διαδικασίας ανάλυσης της ροής από την επίθεση με το wireshark μπορούμε να απομονώσουμε χαρακτηριστικά με την χρήση φίλτρων ώστε να δημιουργήσουμε τους κανόνες. Ο κανόνας που υλοποιήθηκε μέσω αυτού του φίλτρου είναι:

```
1  alert tcp any any → $HOME_NET any (msg"NMAP with -sC DETECTED"; flags:5; sid:1111111;)
```

Η παράμετρος flags: 5 υλοποιεί τα tcp φίλτρα που έχουμε χρησιμοποιήσει στο wireshark.




*Σχήμα 8: Ανάλυση nmap -sW*

Από το manual του nmap μπορούμε να δούμε πως η παράμετρος -sW ελέγχει το μέγεθος παραθύρου της απάντησης οπότε στην ανάλυση στο wireshark εφαρμόζουμε το φίλτρο

- Ip.src == IP του θύματος
- tcp.window_size == 0

Ο κανόνας που δημιουργήθηκε μέσω του φίλτρου είναι:

```
1 alert tcp any any → $HOME_NET any (msg"NMAP with -sw DETECTED"; window:0; sid:1111113;)
```

Η διαδικασίας ανάλυσης μίας επίθεσης μας βοηθάει να αμυνθούμε και να αναβαθμίσουμε τις άμυνες ασφαλείας ενός συστήματος. Αναλύοντας την ροή πακέτων δικτύου μίας επίθεσης δικτύου μπορούμε να δημιουργήσουμε κανόνες σε οποιοδήποτε Σύστημα ανίχνευσής εισβολής, όπως και να επεκτείνουμε τις γνώσεις μας στην ασφάλεια. Η γνώση και η ενημέρωση σε καινούργια συμβάντα και επιθέσεις είναι μία σημαντική τεχνική την οποία εφαρμόζουν όλοι οι επαγγελματίες ασφάλειας.[30]

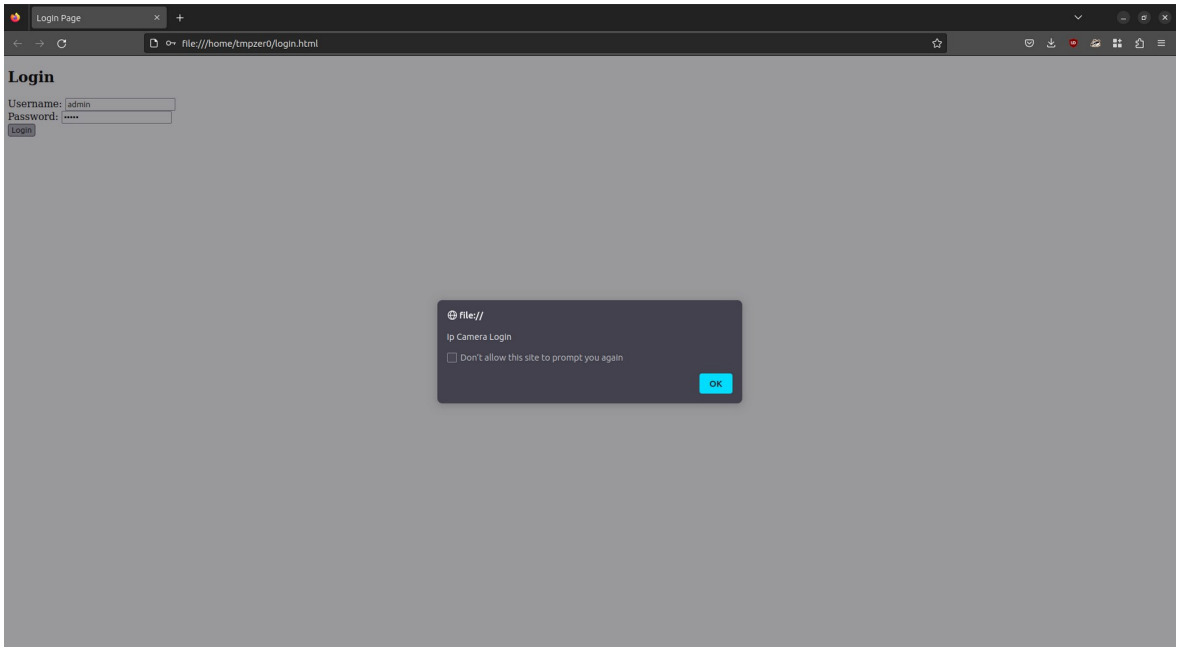
# 7 ΣΥΣΚΕΥΕΣ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

## *7.1 Κάμερες με διεύθυνση IP*

Οι κάμερες IP είναι συσκευές συνδεδεμένες στο δίκτυο που καταγράφουν βίντεο και, σε ορισμένες περιπτώσεις, ήχο και μεταδίδουν τα δεδομένα μέσω του Διαδικτύου ή ενός τοπικού δικτύου. Υπάρχουν νόμοι για την τοποθεσία που μπορούν να τοποθετηθούν ώστε να μην παραβιάζετε το προσωπικό απόρρητο από άλλους ανθρώπους. Χαρακτηριστικά τα οποία διαθέτουν οι καινούριες κάμερες και κατατάσσονται στο Διαδίκτυο των Πραγμάτων:

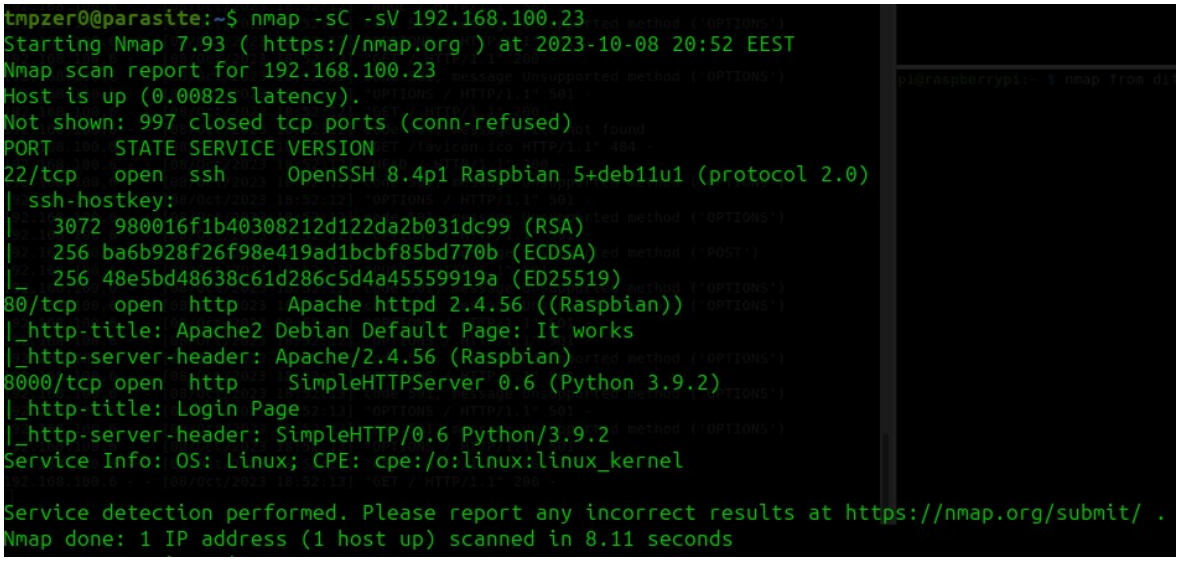
- Οι κάμερες IP είναι εξοπλισμένες με διεπαφές δικτύου (Ethernet ή Wi-Fi) που τους επιτρέπουν να συνδέονται στο διαδίκτυο ή σε τοπικό δίκτυο. Αυτή η συνδεσιμότητα επιτρέπει την απομακρυσμένη πρόσβαση και έλεγχο.
- Καταγράφουν δεδομένα βίντεο και ήχου και τα μεταδίδουν μέσω του δικτύου.
- Ορισμένες κάμερες αποθηκεύουν δεδομένα σε υπηρεσίες cloud.
- Οι κάμερες IP μπορούν να αποτελούν μέρος μεγαλύτερων δικτύων παρακολούθησης, όπου πολλαπλές κάμερες αναπτύσσονται και διαχειρίζονται κεντρικά.

Οι κάμερες είναι ανιχνεύσιμες από το shodan το οποίο λειτουργεί με crawlers. Το login.html είναι ένα παράδειγμα το οποίο υλοποιεί την είσοδο στο σύστημα ελέγχου μίας κάμερας IP. Με την χρήση του snort μπορούμε να έχουμε εξειδικευμένους κανόνες ώστε να γνωρίζουμε αν κάποιος χρήστης προσπάθησε να παραβιάσει την πρόσβαση, παραβίασε την πρόσβαση και βλέπει αποθηκευμένα δεδομένα ή την ροή της κάμερας.




*Σχήμα 9: Παράδειγμα σελίδας εισόδου IP Camera*

Στο Σχήμα 3: Δοκιμή διαφορετικής διεύθυνσης IP βλέπουμε πως το snort δημιούργησε αναφορά για την πόρτα 80 και 8000 οι οποίες υλοποιούσαν υπηρεσία http. Στα αποτελέσματα του nmap μπορούμε να δούμε πως η σάρωση πέρασε από την σελίδα login.html.[24][7]




*Σχήμα 10: Αποτελέσματα nmap*

Με τον ίδιο τρόπο θα μπορούσε να δημιουργηθεί αναφορά από μια μηχανή αναζήτησης όπως το shodan. Οι ενέργειες και οι κανόνες που μπορούν να εφαρμοστούν στο snort μπορούν να μας ενημερώσουν για κάθε πιθανή παραβίαση ή ακόμα και για μία απλή σάρωση χωρίς κακόβουλο σκοπό.

Τα πρωτόκολλα τα οποία υλοποιεί μια κάμερα IP:

- IP
- HTTP/HTTPS
- RTSP
- RTMP
- ONVIF
- UpnP
- FTP
- SMTP
- SNMP
- SSH
- SMB/CIFs

## *7.2 Συσκευές Υγείας*

Το διαδίκτυο των πραγμάτων έχει επηρεάσει σημαντικά και τον κλάδο της υγειονομικής περίθαλψης. Αναπτύσσονται εφαρμογές και ιατρικές συσκευές οι οποίες συλλέγουν και μεταδίδουν δεδομένα που σχετίζονται με την υγεία. Τα υγειονομικά δεδομένα ανήκουν στην κατηγορία των ευαίσθητων δεδομένων και πρέπει να προστατεύονται. Αποτελούν στόχο από κακόβουλους χρήστες διότι η κατοχή τους μπορεί να οδηγήσει σε περισσότερες επιθέσεις.[31]

- Κλοπή ταυτότητας
  - Τα δεδομένα υγείας περιέχουν όνομα, διεύθυνση, ημερομηνία γέννησης, βιομετρικά χαρακτηριστικά τα οποία μπορούν να βοηθήσουν να εκτελεστεί μία επίθεση κλοπής ταυτότητας.
- Επιθέσεις λύτρων
  - Κλοπή ιατρικού ιστορικού
  - Κρυπτογράφηση βάσης δεδομένων νοσοκομείου
- Πώληση δεδομένων
  - Πώληση στην μαύρη αγορά
  - Πώληση σε εταιρίες ασφάλισης
  - Πώληση σε εταιρίες έρευνας

Είναι απαραίτητο οι οργανισμοί υγειονομικής περίθαλψης όπως και οι κατασκευαστές συσκευών υγείας να εφαρμόζουν μέτρα ασφάλειας. Η κρυπτογράφηση, δοκιμές ασφάλειας όπως και οι εκπαίδευση των εργαζομένων είναι μέτρα τα οποία θα πρέπει να εφαρμόζονται πάντα.

Εκτός από τους οργανισμούς υγειονομικής περίθαλψης ερχόμαστε σε επαφή με συσκευές υγείας καθημερινά. Έξυπνα ρολόγια, κινητά και εφαρμογές οι οποίες βοηθάνε τον χρήστη να συντηρεί ιστορικό γυμναστικής δεν έχουν πρωταρχικό στόχο την υγεία, αλλά έχουν επαφή με δεδομένα υγείας οπότε πρέπει να αντιμετωπίζονται με τα ίδια μέτρα ασφάλειας. Συσκευές οι οποίες εξειδικεύονται στην υγεία και συμπεριλαμβάνονται στο διαδίκτυο των πραγμάτων:

- Έξυπνα πιεσόμετρα
  - Παρέχουν ιστορικά δεδομένα και ανάλυση ώστε να διευκολύνουν τον χρήστη να επεξεργαστεί τα αποτελέσματα.
  - Μετρητής γλυκόζης
    - Παρακολουθεί τα επίπεδα γλυκόζης στο αίμα. Οι εφαρμογές που έχουν οι συσκευές επεξεργάζονται το ιστορικό και κάνουν αναλύσεις
  - Αυτόματη χορήγηση φάρμακου
    - Βοηθάν τους ασθενείς να κρατάνε το πρόγραμμα και την δοσολογία των φαρμάκων και χορηγούν αυτόματα την θεραπεία.
  - Ελεγκτές πτώσης
    - Ανιχνεύουν πτώση σε ηλικιωμένους χρήστες ώστε να σταλεί ειδοποίηση σε υπηρεσίες άμεσης ανάγκης.
    - Ανιχνεύουν πτώση σε χρήστες οι οποίοι είναι οδηγοί μηχανής ώστε να ενημερωθεί αυτόματα η αστυνομία και άμεση βοήθεια σε περίπτωση ατυχήματος
  - Αισθητήρες περιβάλλοντος
    - Ελέγχουν ποιότητα αέρα, θερμοκρασία,υγρασία

Βλέπουμε πως ο ρόλος τόσο των συσκευών που επεξεργάζονται δεδομένα υγείας μέσω μίας εφαρμογής όπως και τον συσκευών που δημιουργήθηκαν με σκοπό την υγειονομική περίθαλψη είναι σημαντικός. Τα έξυπνα ρολόγια ελέγχουν συνεχώς την καρδία του χρήστη και τον ενημερώνουν για ανωμαλίες που μπορούν να είναι κρίσιμες. Σε συσκευές υγείας τα μέτρα πρέπει να είναι αυστηρά διότι ο στόχος της επίθεσης μπορεί να είναι η ακεραιότητα του χρήστη.

# 8 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το διαδίκτυο των πραγμάτων έχει εξελιχθεί και συνεχίζει να εξελίσσετε με ταχύ ρυθμό. Είναι αδύνατο οι ρυθμοί ανάπτυξης της ασφάλειας να συμβαδίσουν με τους ρυθμούς ανάπτυξης του διαδικτύου των πραγμάτων. Είδαμε πως με ήδη υπάρχουσες τεχνολογίες μπορούμε όμως να προστατέψουμε τα συστήματα μας. Ο βέλτιστος τρόπος να μειωθεί αυτό το χάσμα, όπως και το χάσμα που υπάρχει ανάμεσα στην τεχνογνωσία του χρήστη και ενός αναλυτή, είναι η ενσωμάτωση του συστήματος ανίχνευσης εισβολής στο διαδίκτυο των πραγμάτων όπως και στην καθημερινότητα του χρήστη. Σαν χρήστες είμαστε εξοικειωμένοι με την χρήση εφαρμογών υγείας όπου μία συσκευή ελέγχει την υγεία μας. Στο επίπεδο υγείας της συσκευής οι μόνες ενημερώσεις που δέχεται ο χρήστης είναι η κατάσταση μνήμης και η λειτουργία της συσκευής. Στο ενδεχόμενο που οι συσκευές υγείας και οι εφαρμογές, αλγοριθμικά λειτουργούσαν μόνο με κριτήρια να υπάρχει παλμός και αναπνοή, οι χρήστες θα θεωρούσαν τις υπηρεσίες που παρέχουν αναξιόπιστες και ελλιπής. Αυτός είναι ο τρόπος που λειτουργεί η υγεία μίας συσκευής. Δεν έχουμε ενημέρωση την στιγμή που γίνετε μία επίθεση, γίνετε καταγραφή στα αρχεία καταγραφής στα οποία είναι δύσκολο να αναγνωρίσουν αναλυτές αρκετές επιθέσεις. Η ανάλυση και η ενημέρωση είναι ο λόγος που οι χρήστες είναι ικανοποιημένοι και αυτό είναι κάτι που πρέπει να εφαρμοστεί στην ασφάλεια του διαδικτύου των πραγμάτων. Τα έξυπνα σπίτια θα πρέπει να υλοποιούν σύστημα ανίχνευσης εισβολής διότι προσθέτουν στο οικείο περιβάλλον του χρήστη συσκευές οι οποίες είναι ευάλωτες, και το σύστημα ανίχνευσης εισβολής προσφέρει λύση. Είναι όμως η βέλτιστη πρώτη επαφή που μπορεί να έχει ένας χρήστης με ένα Επιχειρησιακό Κέντρο Ασφάλειας, κάτι το οποίο θα τον κάνει να ευαισθητοποιηθεί σε θέματα ασφάλειας και να είναι πιο ενήμερος προς τις απειλές.

# 9 ΠΡΟΤΑΣΗ

Τα συστήματα ανίχνευσης εισβολής δικτύου και κεντρικού υπολογιστή είναι ικανά ώστε να ενδυναμώσουν ένα έξυπνο σπίτι και να μειώσουν τις απειλές σε θέματα κυβερνοασφάλειας. Βασικός λόγος αυτής της ανάγκης είναι πως η υλοποίηση ενός έξυπνου σπιτιού συμπεριλαμβάνει ευάλωτες συσκευές. Είναι άξιο να σημειωθεί πως μπορεί να γίνει αναλογία ενός έξυπνου σπιτιού με έναν απλό χρήστη. Ένα έξυπνο σπίτι διαθέτει έναν δρομολογητή που συνδέονται όλες οι συσκευές και μπορεί να προστατευτεί με ένα σύστημα ανίχνευσης εισβολής δικτύου. Ένας χρήστης διαθέτει ένα έξυπνο κινητό στο οποίο συνδέονται όλες οι συσκευές ακόμα και όταν βρίσκετε εκτός σπιτιού. Ακουστικά που υλοποιούν Bluetooth, έξυπνο ρολόι, συσκευές υγείας. Οι συσκευές αυτές είναι ευάλωτες σε ασύρματες επιθέσεις δικτύου. Θα πρέπει να υλοποιηθούν συστήματα ανίχνευσης εισβολής για έξυπνα τηλέφωνα όπως Android, Apple ώστε οι χρήστες να είναι ενήμεροι αν δέχονται επίθεση Man-in-the-middle, de-authentication ή επιθέσεις Bluetooth σε συσκευές υγείας. Ένα σύστημα ανίχνευσης εισβολής με κέντρο ένα τηλέφωνο όχι απλά θα δρα σαν ένα ισχυρό τοίχος προστασίας της συσκευής αλλά θα έχει την δυνατότητα να διασφαλίζει τα δεδομένα του χρήστη που συμπεριλαμβάνουν δεδομένα υγείας και όλες τις συνδεμένες συσκευές. Είναι ένα προληπτικό μέτρο το οποίο προσφέρει ευκολία στον χρήστη και ευαισθητοποίηση στην ασφάλεια. Η ασφάλεια είναι ένας τομέας ο οποίος δεν πρέπει να εγκλωβίζετε ή να εφαρμόζεται κατά περίσταση. Τα δεδομένα και οι συσκευές του χρήστη να είναι ασφαλής εφόσον βρίσκετε στην εμβέλεια του συστήματος ανίχνευσης που έχει υλοποιηθεί στο έξυπνο σπίτι αλλά όταν βγει εκτός εμβέλειας να είναι ευάλωτα. Το μέλλον διαφυλάσσει τεχνολογίες οι οποίες θα συγχωνευτούν στην καθημερινότητα όπως έξυπνα σπίτια, έξυπνα αμάξια. Ένα φορητό σύστημα ανίχνευσης είναι μία αναγκαία επένδυση προς το μέλλον. Όσο πιο κοντά είναι στον χρήστη και στην καθημερινότητα του, τόσο πιο εύκολα θα γίνει η μετάβαση και διασφάλιση σε αυτό το ψηφιακό μέλλον.

# ΑΝΑΦΟΡΕΣ

1: Alan J White, Ben Clark, Blue Team Field Manual, 2017

2: Angela Orebaugh, Snort Cookbook: Solutions and Examples for Snort Administrators, 2005

4: Ben Clark, RTFM: Red Team Field Manual v2, 2022

4: Brian Caswell, Snort Intrusion Detection And Prevention Toolkit, 2007

6: Brijendra Singh, Mohammad Zubair Khan, Applications and Challenges in IoT based Smart Homes, 2021

6: Dafydd Stuttard, The Web Application Hacker’s Handbook: finding and Exploiting Security Flaws, 2011

8: DarkReading, Sangfor, https://www.sangfor.com/blog/cybersecurity/list-of-top-ransomware-attacks-in-2023, 2023,

9: Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting: A Condensed Guide for the Security Operations Team and Threat Hunter, 2019

10: Don Murdoch, Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder., 2014

11: Ethem Mining, Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts. , 2019

11: Fadi Al-Turjman, Hadi Zahmatkesh, Ramiz Shahroze, An overview of security and privacy in smart cities' IoT communications, 10.1002/ett.3677, 2019

12: G. Dayanandam, T. V.Rao, D. Bujji Babu, S. Nalini Durga, DDoS Attacks-Analysis and Prevention, 10.1007/978-981-10-8201-6_1, 2018

13: Harry Kasuma Aliwarga;, Performance comparison of fleet management system using IoT node device based on MQTT and HTTP protocol, 10.1063/5.0003076, 2020

15: Jack V. Rincon, Raspberry Pi 4 For Beginners: Simplified Introduction to Raspberry Pi 4 Programming for Beginners On Windows, IOS, Linux, and More (With 26 Easy To Follow Raspberry Pi 4 Projects), 2021

15: John Matherly, The Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work For You, 2016

17: Joseph Muniz, Gary Mclntyre, Nadhem AlFardan, Security Operations Center: Building, Operating, and Maintaining your SOC, 2015

18: Kerry Cox, Managing Security With Snort and IDS Tools, 2004

18: Laura Chappell, Gerald Combs, Wireshark 101: Essential Skills for Network Analysis (Wireshark Solution), 2017

20: Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A survey, 10.1016/j.comnet.2010.05.010, 2010

21: Manfred Vielberth, Fabian Böhm, Ines Fichtinger, Günther Pernul, Security Operations Center: A systematic Study and Open Challenges, 10.1109/ACCESS.2020.3045514, 2020

22: Maxim Zolotykh, Study of Crawlers of Search Engine 'Shodan.io', 2021

23: Paulino Calderon, Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips, 3rd Edition, 2021

23: Peter Kim, The Hacker Playbook3: Practical Guide To Penetration Testing, 2018

25: Peter McLaren, Gordon Russell, William J. Buchanan, Zhiyuan Tan, Decrypting live SSH traffic in virtual environments, 1016/JDIIN.2019.03.010, 2019

25: RaviTeja Gaddam, M. Nandhini, An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment, 10.1109/ICICCT/2017.7975177, 2017

27: Santiago Figueroa Lorenzo, Javier Añorga Benito, Pablo García Cardarelli, Jon Alberdi Garaia, Saioa Arrizabalaga Juaristi, A Comprehensive Review of RFID and Bluetooth Security: Practical Analysis, 10.3390/technologies7010015, 2019

27: SH Kok, Azween Abdullah, NZ Jhanhji, Mahadevan Supramaniam, Ransomware, Threat and Detection Techniques: A Review, 197868067, 2019

28: Yazdan Ahmad Qadri, Ali Nauman, Yousaf Bin Zirkia, Athanasios V. Vasilakos, Sung Won Kim, The Future of Healthcare Internet of Things: A survey of Emerging Technologies, 10.1109/COMST.2020.2973314, 2018

29: Zhimin Zhou, Zhongwen Chen, Tiecheng Zhou, Xiohui Guan, The study on network intrusion detection system of Snort, 978-1-4244-5162-3, 2010

31: Zia Uddin Ahmed, Mohammad Golam Mortuza, Mohammed Jashim Uddin, Md. Humayun Kabir, Md. Mahiuddin, MD. Jiabul Hoque, Internet of Things Based Patient Health Monitoring System Using Wearable Biomedical Device, 987-1-5386-5230-5, 2019

32: İlayda Gündoüdu, Ali Aydın Selçuk, Süleyman özarslan, Effectiveness Analysis of Public Rule Sets Used in Snort Intrusion Detection System, 978-1-6654-3649-6, 2021

# 10 ΠΑΡΑΡΤΗΜΑΤΑ ΚΩΔΙΚΑ

## Login.html

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Login Page</title>
</head>
<body>
    <div>
        <h2>Login</h2>
        <form onsubmit="checkCredentials(); return false;">
            <div>
                <label for="username">Username:</label>
                <input type="text" id="username" name="username" required>
            </div>
            <div>
                <label for="password">Password:</label>
                <input type="password" id="password" name="password" required>
            </div>
            <div>
                <input type="submit" value="Login">
            </div>
        </form>
    </div>

    <script>
        function checkCredentials() {
            var username = document.getElementById('username').value;
```

```
29          var password = document.getElementById('password').value;
30
31          if (username === 'admin' && password === 'admin') {
32              alert('Ip Camera Login');
33          }
34      }
35  </script>
36 </body>
37 </html>
```

# 11 ΟΔΗΓΟΣ ΧΡΗΣΗΣ ΛΟΓΙΣΜΙΚΟΥ

## *11.1 Εγκατάσταση Raspbian*

Λήψη του λογισμικού από την επίσημη σελίδα Raspberry Pi.

Εισαγωγή κάρτας SD ώστε να γίνει εγγραφή της εικόνας

Εύρεση του device της κάρτας SD

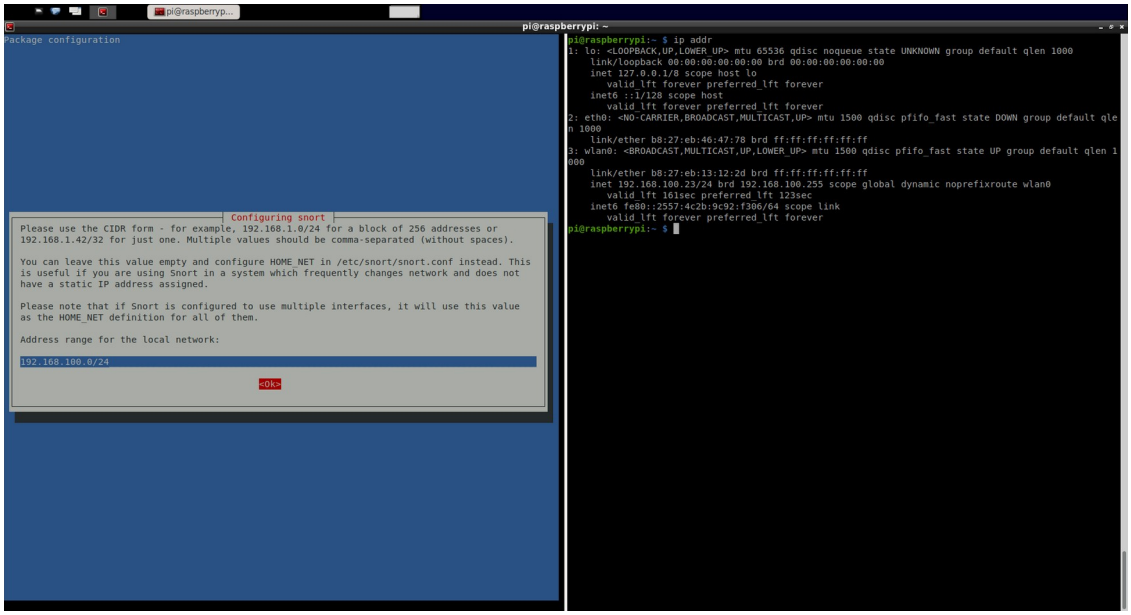
```
1 sudo fdisk -l
2 sudo dd bs=4M if=<raspberry pi image> of=/dev/<sd_device> status=progress conv=fsync
```

Εισαγωγή της κάρτας SD στο Raspberry Pi.

Η εκκίνηση του Raspberry PI γίνετε με την έναρξη τροφοδοσίας.

### *11.2 Εγκατάσταση Snort*

```
1 sudo apt-get update

2 sudo apt-get upgrade

3  sudo apt install build-essential libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev luajit hwloc libdnet-dev libdumbnet-dev bison flex liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev libmnl-dev autotools-dev libluajit-5.1-dev libunwind-dev

4 sudo apt-get install snort
```



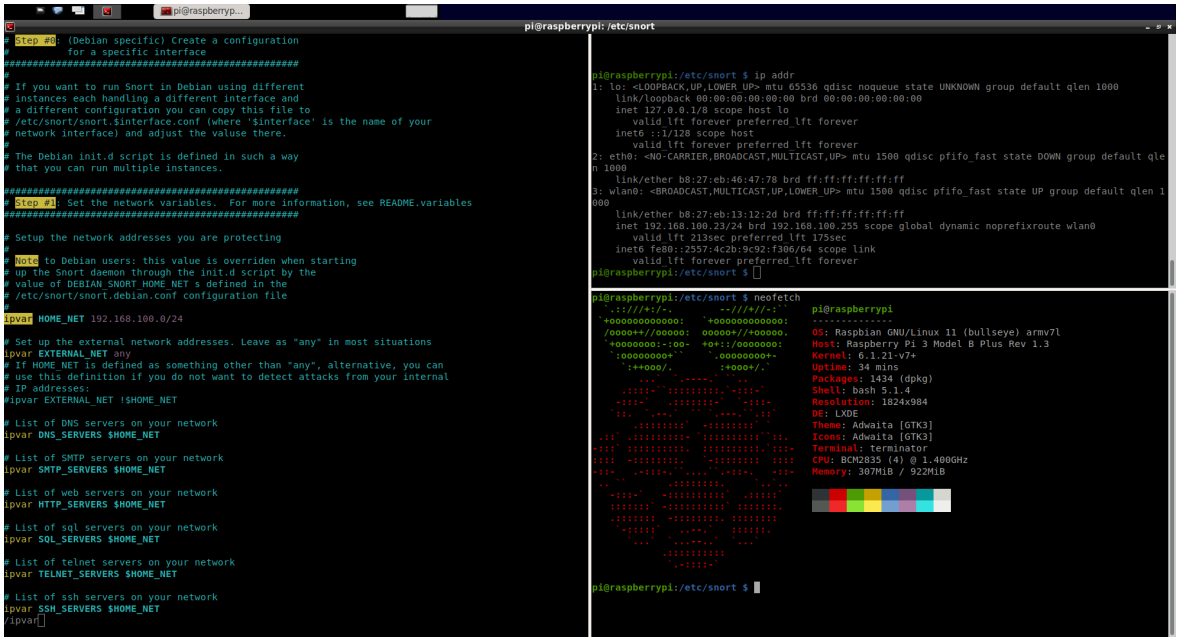

*Σχήμα 11: Ρυθμίσεις δικτύου Snort*

Κατά την εγκατάσταση του Snort θα μας ζητηθεί να ορίσουμε το εύρος των διευθύνσεων IP τις οποίες θα χρησιμοποιήσει το Snort.

Εντολές δοκιμής του Snort

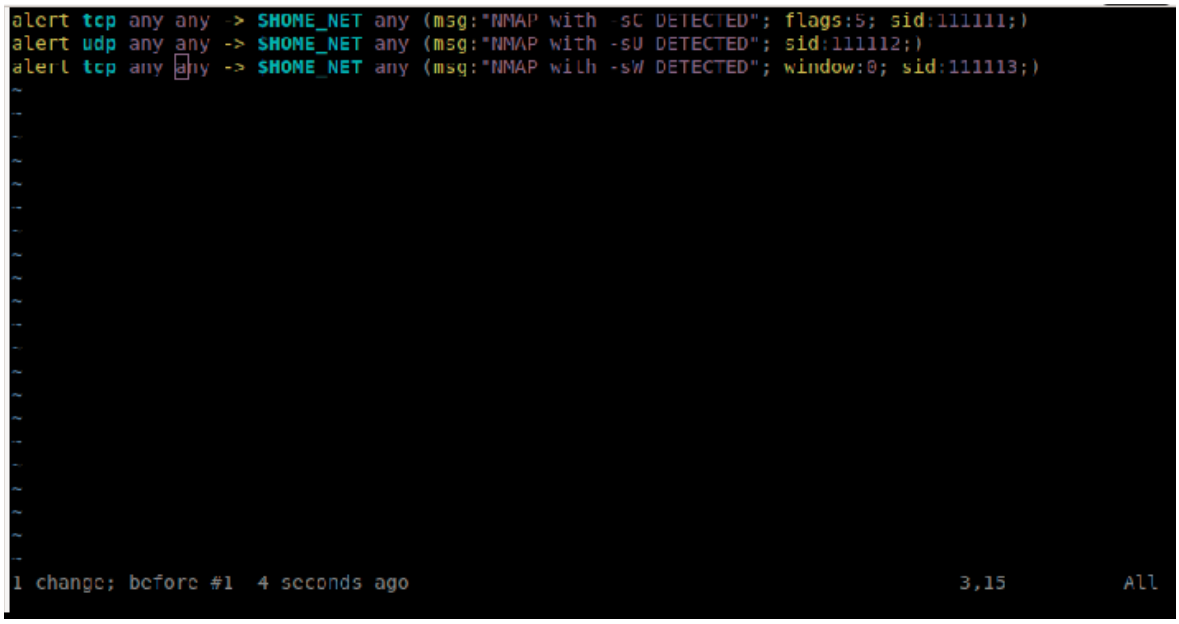
```
systemctl status snort

sudo snort -T -i <interface> -c /etc/snort/snort.conf
```

**Με την ολοκλήρωση της εγκατάστασης θα πρέπει να οριστεί η μεταβλητή ipvar HOME_NET με την τιμή της IP στο αρχείο /etc/snort/snort.conf. Το συγκεκριμένο αρχείο είναι υπεύθυνο για τους κανόνες τους οποίους ορίζουμε.**




*Σχήμα 12: Αρχείο διαχείρισης*

### *11.3 Κανόνες Snort*




*Σχήμα 13: Κανόνες Snort*

### *11.4 Εγκατάσταση Terminator*

Το terminator είναι ένα τερματικό του Linux. Η επιλογή του έγινε διότι προσφέρει ευελιξία και διαχωρισμό παραθύρων που κάνει εύκολη την δουλεία του αναλυτή προσφέροντας γρήγορα περισσότερη πληροφορία

```
1  sudo apt-get install terminator
```

### *11.5 Εγκατάσταση Nmap*

```
1  sudo apt-get install nmap
```

Χρήσιμες τεχνικές σάρωσης:

- -sS

- Ξεκινάει μια σύνδεση TCP στέλνοντας ένα πακέτο SYN
- Εάν η απάντηση είναι SYN/ACK η θύρα είναι ανοιχτή
- Εάν η απάντηση είναι RST/ACK η θύρα είναι κλειστή

- -sT
  - Ξεκινάει μια πλήρη σύνδεση TCP
  - Εάν η απάντηση είναι SYN/ACK η θύρα είναι ανοιχτή
  - Εάν η απάντηση είναι RST/ACK η θύρα είναι κλειστή
- -sU
  - Σάρωση ανοιχτών θυρών που υλοποιούν UDP
  - High ports
  - Στέλνει πακέτα UDP
- -sA
  - Στέλνει ένα πακέτο ACK
  - Χρησιμοποιείται για έλεγχος τείχους προστασίας
- -sW
  - Εξετάζει το μέγεθος του παραθύρου TCP
- -sN
  - Στέλνει ενα πακέτο TCP χωρίς να είναι ορισμένα τα flags
- -sF
  - Στέλνει ένα πακέτο TCP με ενεργό FIN flag
- -sX
  - Στέλνει ένα πακέτο με ενεργά τα flag FIN, URG, PUSH
- -sP
  - Στέλνει πακέτα ICMP ping

- -sV
    - Ελέγχει και αναγνωρίζει τις υπηρεσίες

Είναι σημαντικό να σημειωθεί πως ανάλογα τις παραμέτρους του nmap δημιουργούνται οι ανάλογοι κανόνες στο snort.

| Name | Classification |
|---|---|
| address-info | default safe |
| afp-serverinfo | default discovery safe |
| ajp-auth | default auth safe |
| ajp-methods | default safe |
| amqp-info | default discovery safe version |
| auth-owners | default safe |
| backorifice-info | default discovery safe |
| bitcoinrpc-info | default discovery safe |
| cassandra-info | default discovery safe |
| clock-skew | default safe |
| creds-summary | auth default safe |
| dicom-ping | discovery default safe auth |
| dns-nsid | discovery default safe |
| dns-recursion | default safe |
| dns-service-discovery | default discovery safe |
| epmd-info | default discovery safe |
| finger | default discovery safe |
| flume-master-info | default discovery safe |

| Name | Classification |
|---|---|
| | |
| freelancer-info | default discovery safe version |
| ftp-anon | default auth safe |
| ftp-bounce | default safe |
| ftp-syst | default discovery safe |
| ganglia-info | default discovery safe |
| giop-info | default discovery safe |
| gopher-ls | default discovery safe |
| hadoop-datanode-info | default discovery safe |
| hadoop-jobtracker-info | default discovery safe |
| hadoop-namenode-info | default discovery safe |
| hadoop-secondary-namenode-info | default discovery safe |
| hadoop-tasktracker-info | default discovery safe |
| hbase-master-info | default discovery safe |
| hbase-region-info | default discovery safe |
| hddtemp-info | default discovery safe |
| hnap-info | safe discovery default version |
| http-auth | default auth safe |
| http-cisco-anyconnect | default discovery safe |
| http-cookie-flags | default safe vuln |
| http-cors | default discovery safe |
| http-favicon | default discovery safe |

| Name | Classification |
|---|---|
| http-generator | default discovery safe |
| http-git | default safe vuln |
| http-ls | default discovery safe |
| http-methods | default safe |
| http-ntlm-info | default discovery safe |
| http-open-proxy | default discovery external safe |
| http-robots.txt | default discovery safe |
| http-svn-enum | default discovery safe |
| http-svn-info | default discovery safe |
| http-title | default discovery safe |
| http-webdav-scan | safe discovery default |
| ike-version | default discovery safe version |
| imap-capabilities | default safe |
| imap-ntlm-info | default discovery safe |
| ip-https-discover | discovery safe default |
| ipv6-node-info | default discovery safe |
| irc-info | default discovery safe |
| iscsi-info | default safe discovery |
| jdwp-info | default safe discovery |
| knx-gateway-info | default discovery safe |
| maxdb-info | default version safe |
| mongodb-databases | default discovery safe |

| Name | Classification |
|---|---|
| mongodb-info | default discovery safe |
| ms-sql-info | default discovery safe |
| ms-sql-ntlm-info | default discovery safe |
| mysql-info | default discovery safe |
| nat-pmp-info | default discovery safe |
| nbns-interfaces | default discovery safe |
| nbstat | default discovery safe |
| ncp-serverinfo | default discovery safe |
| netbus-info | default discovery safe |
| nntp-ntlm-info | default discovery safe |
| ntp-info | default discovery safe |
| openflow-info | default safe |
| openlookup-info | default discovery safe version |
| p2p-conficker | default safe |
| pop3-capabilities | default discovery safe |
| pop3-ntlm-info | default discovery safe |
| quake1-info | default discovery safe version |
| quake3-info | default discovery safe version |
| quake3-master-getservers | default discovery safe |
| rdp-ntlm-info | default discovery safe |
| rmi-dumpregistry | default discovery safe |
| rpcinfo | discovery default safe version |

| Name | Classification |
|---|---|
| rtsp-methods | default safe |
| servicetags | default discovery safe |
| sip-methods | default safe discovery |
| smb-os-discovery | default discovery safe |
| smb-security-mode | default discovery safe |
| smb2-security-mode | safe discovery default |
| smb2-time | discovery safe default |
| smtp-commands | default discovery safe |
| smtp-ntlm-info | default discovery safe |
| snmp-hh3c-logins | default discovery safe |
| snmp-info | default version safe |
| snmp-interfaces | default discovery safe |
| snmp-netstat | default discovery safe |
| snmp-processes | default discovery safe |
| snmp-sysdescr | default discovery safe |
| snmp-win32-services | default discovery safe |
| snmp-win32-shares | default discovery safe |
| snmp-win32-software | default discovery safe |
| snmp-win32-users | default auth safe |
| socks-auth-info | discovery safe default |
| socks-open-proxy | default discovery external safe |
| ssh-hostkey | safe default discovery |

| Name | Classification |
|---|---|
| sshv1 | default safe |
| ssl-cert | default safe discovery |
| ssl-date | discovery safe default |
| ssl-known-key | safe discovery vuln default |
| sslv2 | default safe |
| sstp-discover | discovery default safe |
| telnet-ntlm-info | default discovery safe |
| tls-alpn | discovery safe default |
| tls-nextprotoneg | discovery safe default |
| ubiquiti-discovery | default discovery version safe |
| upnp-info | default discovery safe |
| uptime-agent-info | safe default |
| ventrilo-info | default discovery safe version |
| vnc-info | default discovery safe |
| wdb-version | default safe version discovery vuln |
| weblogic-t3-info | default safe discovery version |
| wsdd-discover | safe discovery default |
| x11-access | default safe auth |
| xmlrpc-methods | default safe discovery |
| xmpp-info | default safe discovery version |