ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
Τμήμα Ηλεκτρολόγων & Ηλεκτρονικών Μηχανικών
www.eee.uniwa.gr
Θηβών 250, Αθήνα-Αιγάλεω 12241
Τηλ. +30 210 538-1225, Fax. +30 210 538-1226

UNIVERSITY of WEST ATTICA
FACULTY OF ENGINEERING
Department of Electrical & Electronics Engineering
www.eee.uniwa.gr
250, Thivon Str., Athens, GR-12241, Greece
Tel:+30 210 538-1225, Fax:+30 210 538-1226

Πρόγραμμα Μεταπτυχιακών Σπουδών
Διαδικτυωμένα Ηλεκτρονικά Συστήματα

Master of Science in
Internetworked Electronic Systems

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τεχνολογίες αξιολόγησης της ασφάλειας σε ενσωματωμένα συστήματα βασισμένα σε IoT τεχνολογίες και πύλες δικτύου:

Μελέτη μέσω κατάλληλου λογισμικού ανοιχτού κώδικα σε δοκιμές διείσδυσης σε υλικό και λογισμικό.

Μεταπτυχιακός Φοιτητής: Φαλούτσος Βασίλειος, ΑΜ: IES-0045

Επιβλέπων: Παναγιώτης Παπαγέωργας, Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, ΙΟΥΝΙΟΣ 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
Τμήμα Ηλεκτρολόγων & Ηλεκτρονικών Μηχανικών
www.eee.uniwa.gr
Θηβών 250, Αθήνα-Αιγάλεω 12244
Τηλ. +30 210 538-1225, Fax. +30 210 538-1226

UNIVERSITY of WEST ATTICA
FACULTY OF ENGINEERING
Department of Electrical & Electronics Engineering
www.eee.uniwa.gr
250, Thivon Str., Athens, GR-12244, Greece
Tel:+30 210 538-1225, Fax:+30 210 538-1226

Πρόγραμμα Μεταπτυχιακών Σπουδών
Διαδικτυωμένα Ηλεκτρονικά Συστήματα

Master of Science in
Internetworked Electronic Systems

MSc Thesis

Security assessment technologies in embedded systems based on IoT technologies and Gateways:
Study through appropriate open source software in hardware and software penetration tests.

Postgraduate student: Faloutsos Vasileios Reg. Nr.: IES-0045

MSc Thesis Supervisor: Prof. Papageorgas Panagiotis

ATHENS-EGALEO, JUNE 2021

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας μεταπτυχιακής εργασίας αποτελούν οι τεχνολογίες αξιολόγησης της ασφάλειας σε ενσωματωμένα συστήματα βασισμένα σε IoT τεχνολογίες και σε πύλες δικτύου. Στο αρχικό στάδιο περιγράφονται τα ενσωματωμένα συστήματα μικρής μεσαίας και μεγάλης κλίμακας και αναλύεται η θεωρητική βάση του IoT και των πυλών δικτύου, τα μοντέλα επικοινωνίας τους καθώς και η διασύνδεσή των smart things και των sensors. Ιδιαίτερη έμφαση της εργασίας δίνεται στα πρότυπα της ασφάλειας όπως αυτά ορίζονται τόσο από διεθνείς οργανισμούς όπως ο Enisa (European Union Agency for Cybersecurity) όσο και από την Εθνική Στρατηγική Κυβερνοασφάλειας του Ελληνικού Υπουργείου Ψηφιακής Διακυβέρνηση. Σε συνέχεια των προδιαγραφών αναφέρονται οι κατευθυντήριες γραμμές για την διασφάλιση της ασφάλειας IOT και οι απειλές σε όλη την αλυσίδα εφοδιασμού. Παρουσιάζονται και αναλύονται οι καλές πρακτικές για την βελτίωση της διασφάλιση της ασφάλειας της αλυσίδας IOT.
Μελετώνται μέσω κατάλληλου λογισμικού ανοιχτού κώδικα δοκιμές διείσδυσης σε υλικό και λογισμικό. Αυτό επιτυγχάνεται με την χρήση των λειτουργικών συστημάτων ανοιχτού κώδικα Oracle VM VirtualBox, Kali Linux βασισμένη στο Debian, το OWASP ZAP (Zed Attack Proxy) γνωστός ως "man-in-the-middle proxy" και το OWASP BWA που είναι μία ευάλωτη εικονική μηχανή και φιλοξενείται στο SourceForge, ένα δημοφιλές αποθετήριο για έργα ανοιχτού κώδικα. Σκοπός της μεταπτυχιακής εργασίας είναι η διερεύνηση των ευπαθειών (Vulnerabilities) των συστημάτων και η ανάδειξη της αναγκαιότητας των καλών πρακτικών ασφαλείας για την αποφυγή και πρόληψη των ευπαθειών.

ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ: Ενσωματωμένα Συστήματα, Διαδίκτυο των Πραγμάτων, Πύλες Δικτύου, Σύννεφο, Έξυπνα Πράγματα, Αισθητήρια, Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών, Εθνική Στρατηγική Κυβερνοασφάλειας, Υπουργείο Ψηφιακής Διακυβέρνησης, Τεχνολογία Πληροφοριών και Επικοινωνίας, Κυβερνοχώρος, Κυβερνοαπειλές, Κυβερνοασφάλεια, Δοκιμές Διείσδυσης

ABSTRACT

The subject of this master's thesis are security assessment technologies in embedded systems based on IoT technologies and gateways. The initial stage describes the small, medium and large scale of Embedded Systems and analyzes the IoT and Gateways, the communication models as well as the interconnection of Smart things and Sensors. Emphasis is given to security standards as defined by both international organizations such as Enisa (European Union Agency for Cybersecurity) and the National Cybersecurity Strategy of the Greek Ministry of Digital Government. The specifications are followed by guidelines for ensuring IoT security and threats throughout the supply chain. Good practices for improving the security of the IoT chain are presented and analyzed.

Hardware and software penetration tests are studied through appropriate open source software. This is achieved by using open source operating systems such as Oracle VM VirtualBox, Kali Linux based on Debian, OWASP ZAP (Zed Attack Proxy) known as the "man-in-the-middle proxy" and OWASP BWA which is a vulnerable virtual machine hosted on SourceForge, a popular repository for open source projects. The purpose of the master's thesis is to investigate the vulnerabilities of the systems and to highlight the need for good security practices to avoid and prevent vulnerabilities.

Keywords : Embedded Systems, Internet of things (IOT), Gateways, Cloud, Smart things, Sensors, European Union Agency for Cybersecurity (Enisa), National Cybersecurity Strategy, Ministry of Digital Governance, Information and Communication Technology (ICT), Cyber, Cyberthreats, Cybersecurity, Penetration Tests

0 Εισαγωγή

Η παρούσα εργασία έχει ως αντικείμενο τη μελέτη τεχνολογιών αξιολόγησης της ασφάλειας σε ενσωματωμένα συστήματα βασισμένα σε IoT τεχνολογίες και πύλες δικτύου και μέσω κατάλληλου λογισμικού ανοιχτού κώδικα τις δοκιμές διείσδυσης σε υλικό και λογισμικό.
Στο πρώτο κεφάλαιο γίνεται αναφορά στα ενσωματωμένα συστήματα (Embedded Systems), στα χαρακτηριστικά τους και το εύρος εφαρμογής τους.
Στο δεύτερο κεφάλαιο γίνεται περιγραφή του Διαδικτύου των Πραγμάτων (IOT) και ανάλυση των μοντέλων επικοινωνίας.
Στο τρίτο κεφάλαιο αναφέρονται οι τομείς που βρίσκει εφαρμογή το IOT και γίνεται φανερό το μεγάλο εύρος εφαρμογής του σε πολλούς τομείς.
Στο τέταρτο κεφάλαιο παρουσιάζονται οι αναδυόμενες τεχνολογίες οι οποίες με τη ραγδαία ανάπτυξή τους τα τελευταία χρόνια έχουν συνεισφέρει στην IOT. Τεχνολογία.
Στο πέμπτο κεφάλαιο γίνεται αναφορά του όρου Κυβερνοχώρος και ανάλυση των παραγόντων και των τύπων απειλών για την ασφάλεια IOT
Στο έκτο κεφάλαιο αναλύονται οι κατευθυντήριες γραμμές από διεθνής και ευρωπαϊκούς οργανισμούς για την διασφάλιση ασφάλειας στην αλυσίδα ανεφοδιασμού IOT.
Στο έβδομο κεφάλαιο γίνεται ανάλυση των ειδών των απειλών που αντιμετωπίζονται στην αλυσίδα ανεφοδιασμού.
Στο όγδοο κεφάλαιο αναφέρονται οι τεχνολογίες και οι μηχανισμοί για την διασφάλιση της ασφάλειας στην αλυσίδα ανεφοδιασμού IOT.
Στο ένατο κεφάλαιο γίνονται δοκιμές διείσδυσης (Penetration Tests) μέσω λογισμικού ανοιχτού κώδικα, ώστε να βρεθούν τρωτά σημεία (Vulnerabilities) σε κεντρικό domain.

1 Ενσωματωμένα Συστήματα

Η ενότητα για τα ενσωματωμένα συστήματα αποτελείται από τρεις υποενότητες: Στην πρώτη υποενότητα αναλύονται οι ορισμοί των ενσωματωμένων συστημάτων σύμφωνα με την υπάρχουσα βιβλιογραφία και τους κατασκευαστές. Στη δεύτερη υποενόετητα παρουσιάζονται τα κοινά χαρακτηριστικά και το εύρος εφαρμογών των ενσωματωμένων συστημάτων. Στην τρίτη υποενότητα περιγράφονται οι δυνατότητες του τελικού χρήστη.

1.1 Ορισμοί Ενσωματωμένων Συστημάτων

Οι ορισμοί για τα Ενσωματωμένα Συστήματα (Embedded Systems) σύμφωνα με την βιβλιογραφία και τους κατασκευαστές διατυπώνεται με διαφορετικές προσεγγίσεις. Τα ενσωματωμένα συστήματα διαθέτουν την ίδια αρχιτεκτονική με τα τυπικά υπολογιστικά συστήματα, και αποτελούνται από ένα ή και περισσότερους επεξεργαστές, μνήμη και περιφερειακές συσκευές εισόδου και εξόδου. Το πεδίο εφαρμογής τους συνίσταται στην ικανότητα τους να εκτελούν λειτουργίες σε ένα μηχανικό ή ηλεκτρικό σύστημα. Για να καταστεί αυτό δυνατό χρησιμοποιούν διαφορετικού τύπου επεξεργαστές με περισσότερες δυνατότητες διασυνδέσεων με πολύ λιγότερους πόρους, για αυτό και ονομάζονται μικροεπεξεργαστές.

Εικόνα 1 Ένα ενσωματωμένο σύστημα σε μια κάρτα plug-in με επεξεργαστή, μνήμη, τροφοδοτικό και εξωτερικές διεπαφές [1]

Σύμφωνα με τον *Steve Heath* (2003) υπάρχουν πολλοί ορισμοί για αλλά ο καλύτερος τρόπος να τα ορίσεις είναι να περιγράψεις τι είναι και τι δεν είναι και πως χρησιμοποιείται. Ένα ενσωματωμένο σύστημα είναι ένα σύστημα με μικροεπεξεργαστή που έχει κατασκευαστεί για να ελέγχει μια λειτουργία ή ένα εύρος λειτουργιών. Δεν είναι σχεδιασμένος να προγραμματίζεται από τον τελικό χρήστη όπως αυτό πραγματοποιείται με τον συμβατικό ηλεκτρονικό υπολογιστή.[2]

Κατά τους *Michael Barr* και *Anthony Massa* (2006) ένα ενσωματωμένο σύστημα είναι συνδυασμός υλικού και λογισμικού ηλεκτρονικού υπολογιστή και ενδεχόμενα επιπρόσθετα μέρη, είτε ηλεκτρικά είτε μηχανικά σχεδιασμένα να εκτελούν μία εξειδικευμένη λειτουργία.

Συνεπώς με τον όρο ενσωματωμένα συστήματα προσδιορίζονται τα υπολογιστικά συστήματα υλικού και κλειστού τύπου λογισμικού με ειδικό σχεδιασμό ώστε να εκτελούν αδιαλείπτως κάποια συγκεκριμένη λειτουργία.[3]

Στον προσδιορισμό της έννοιας μπορούν σύμφωνα με τον *Jiacun Wang (2017)* να ταξινομηθούν με βάση την πολυπλοκότητα και την απόδοσή τους σε μικρής κλίμακας, μεσαίας και μεγάλης κλίμακας. Τα συστήματα **μικρής κλίμακας** εκτελούν απλές λειτουργίες με low-end 8- ή 16-bit μικροεπεξεργαστές ή μικροελεγκτές. Τα κύρια εργαλεία προγραμματισμού για την ανάπτυξη ενσωματωμένου λογισμικού για ενσωματωμένα συστήματα μικρής κλίμακας, είναι ένας editor, ένας assembler, ένας cross-assembler και ένα ολοκληρωμένο περιβάλλον ανάπτυξης (IDE). Αυτά τα συστήματα δεν διαθέτουν λειτουργικό σύστημα. Τα συστήματα **μεσαίας κλίμακας** έχουν πολυπλοκότητα υλικού και λογισμικού και χρησιμοποιούν μικροεπεξεργαστές ή μικροελεγκτές 16- ή 32-bit. Για ανάπτυξη ενσωματωμένου λογισμικό στα ενσωματωμένα συστήματα μεσαίας κλίμακας χρησιμοποιούνται οι γλώσσες προγραμματισμού C, C ++, JAVA, Visual C ++, προγράμματα εντοπισμού σφαλμάτων, εργαλείο source-code engineering, simulator (προσομοιωτής) και IDE. Διαθέτουν υποστήριξη λειτουργικού συστήματος. Τα **μεγάλης κλίμακας** ή εξελιγμένα ενσωματωμένα συστήματα διαθέτουν τεράστιο υλικό και πολυπλοκότητες λογισμικού, οι οποίες είναι κατασκευασμένες γύρω από μικροεπεξεργαστές 32- ή 64-bit ή μικροελεγκτές, μαζί με μια σειρά άλλων ενσωματωμένων υψηλής ταχύτητας κυκλωμάτων. Απαιτούνται για εφαρμογές αιχμής που χρειάζονται υλικό και τεχνικές κωδικοποίησης λογισμικού.[5]

Μία άλλη ταξινόμηση είναι τα ενσωματωμένα συστήματα σε πραγματικό χρόνο και σε μη πραγματικό χρόνο. Τα συστήματα σε πραγματικό χρόνο σύμφωνα με τον *Jiacun Wang (2017)* απαιτούν να γίνεται ο υπολογισμός και η παράδοση σωστών αποτελεσμάτων εντός καθορισμένης χρονικής περιόδου, δηλαδή για μια εργασία σε πραγματικό χρόνο το σύστημα έχει προθεσμία. Εάν τα αποτελέσματα είναι εκτός χρονικών ορίων, τότε το αποτέλεσμα είναι άχρηστο, ακόμη και αν είναι σωστό. Τα ενσωματωμένα συστήματα που δεν είναι σε πραγματικό χρόνο ενδέχεται να έχουν επίσης χρονικούς περιορισμούς αλλά το είδος των περιορισμών είναι μόνο ένα μέτρο για απόδοση του συστήματος[4]. Η ραγδαία ανάπτυξη στην τεχνολογία των πληροφοριών, των επικοινωνιών και του Διαδικτύου των πραγμάτων θα οδηγήσει τα ενσωματωμένα συστήματα πραγματικού χρόνου να μετατρέψουν τα αντικείμενα-πράγματα σε έξυπνα (smart things).[5]

1.2 Κοινά χαρακτηριστικά και εύρος εφαρμογών

Τα κοινά χαρακτηριστικά των ενσωματωμένων συστημάτων είναι οι υψηλές ταχύτητες, το μικρό μέγεθος, η πολύ χαμηλή κατανάλωση ενέργειας, η αξιοπιστία, η ακρίβεια, η προσαρμοστικότητα και το μικρό κόστος. Ένας παράγοντας που περιπλέκει την χρήση των ενσωματωμένων συστημάτων είναι ο περιορισμός πόρων επεξεργασίας, που τα καθιστά πιο δύσκολο να προγραμματιστούν και να αλληλοεπιδρούν.[1] Ωστόσο, με την οικοδόμηση

μηχανισμών πληροφοριών πάνω από το υλικό και εκμεταλλευόμενοι τους υπάρχοντες αισθητήρες και την ύπαρξη ενός δικτύου ενσωματωμένων μονάδων, είναι εφικτή η άριστη διαχείριση των διαθέσιμων πόρων σε επίπεδο μονάδας και δικτύου. Με αυτή την μέθοδο υπάρχει βελτιστοποίηση των λειτουργιών.

Σύμφωνα με τον *Jiacun Wang* (2017) *τα* ενσωματωμένα συστήματα σε πραγματικό χρόνο έχουν πεδίο εφαρμογής σε όλο το εύρος ηλεκτρονικών συσκευών όπως: στα αυτοκίνητα, τα κινητά τηλέφωνα, στους προσωπικούς ψηφιακούς βοηθούς (PDA), τα ρολόγια, τις τηλεοράσεις και στις οικιακές ηλεκτρικές συσκευές. Υπάρχουν επίσης μεγαλύτερα και πιο περίπλοκα σε πραγματικό χρόνο ενσωματωμένα συστήματα, όπως τα συστήματα ελέγχου εναέριας κυκλοφορίας, βιομηχανικής διαδικασίας, τα δικτυακά συστήματα πολυμέσων και η βάση δεδομένων σε πραγματικό χρόνο.[5]

Τα ενσωματωμένα συστήματα μπορεί να είναι μέρος ενός ηλεκτρονικού υπολογιστή όπως τα περιφερειακά του το πληκτρολόγιο, ο εκτυπωτής και πολλές άλλες συσκευές. Το εύρος εφαρμογής τους είναι μεγάλο από μία μικρή ηλεκτρονική συσκευή έως ένα μεγάλο υπολογιστικό σύστημα διαθέτοντας περισσότερους του ενός μικροεπεξεργαστή , περιφερειακές μονάδες ελέγχου και δυνατότητα δικτύωσης. Η αναγκαιότητα των ενσωματωμένων συστημάτων αποδεικνύεται με την παραγωγή δισεκατομμυρίων μικροεπεξεργαστών για τα ενσωματωμένα συστήματα, ενώ η παραγωγή επεξεργαστών για τυπικά υπολογιστικά συστήματα κυμαίνονται σε μεγέθη εκατομμυρίων.[6]

1.3 Δυνατότητες τελικού χρήστη

Οι χρήστες ενώ χρησιμοποιούν καθημερινά κάποιο υπολογιστικό σύστημα όπως σταθερό υπολογιστή και φορητό και κάποιες δεκάδες ενσωματωμένων συστημάτων τους είναι εντελώς άγνωστη η ύπαρξη των ενσωματωμένων συστημάτων. Ο τελικός χρήστης συνεπώς δεν έχει την δυνατότητα προγραμματισμού του συστήματος αλλά για την εκάστοτε εφαρμογή έχει σε ορισμένες περιπτώσεις την δυνατότητα να αλλάζει κάποιες παραμέτρους αλλά δεν μπορεί να αλλάξει εξολοκλήρου την λειτουργία του συστήματος που σχεδιάστηκε να εκτελεί.

Σημαντικό είναι να δώσουμε έμφαση στο διαχωρισμό εννοιών μεταξύ ενσωματωμένων συστημάτων και ηλεκτρονικών υπολογιστών. Στον ηλεκτρονικό υπολογιστή ο χρήστης μπορεί να τον χρησιμοποιεί για πάρα πολλές λειτουργίες, εγκαθιστώντας προγράμματα για την εργασία του, την ψυχαγωγία του, να αλληλοεπιδρά με τα μέσα κοινωνικής δικτύωσης για αυτόν τον λόγο ονομάζονται υπολογιστές γενικού σκοπού. Τα ενσωματωμένα συστήματα χρησιμοποιούν διαφορετικού τύπου επεξεργαστές με περισσότερες δυνατότητες διασυνδέσεων με πολύ λιγότερους πόρους, όπως ειπώθηκε σε προηγούμενη παράγραφο.

2 Το Διαδίκτυο των Πραγμάτων και Πύλες Δικτύου

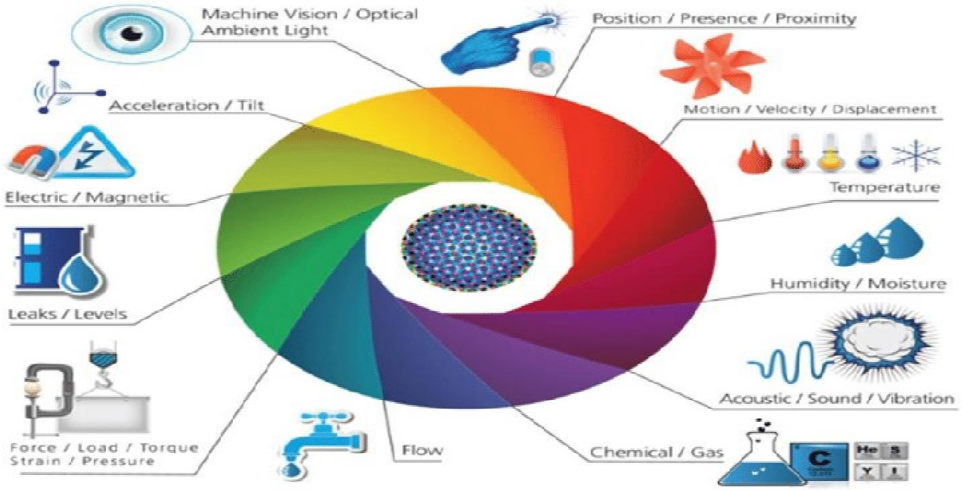
Το διαδίκτυο των πραγμάτων ευρέως γνωστό με τον όρο IoT (Internet of Things) είναι μία από τις κορυφαίες τεχνολογίες της εποχής μας. Σκοπός της συγκεκριμένης ενότητας είναι η

παρουσίαση των ορισμών του διαδικτύου τόσο από την υπάρχουσα βιβλιογραφία όσο και από τους διεθνείς οργανισμούς τυποποίησης και ενώσεις τηλεπικοινωνίων και ασφάλειας δικτύων καθώς και η ανάλυση των μοντέλων επικοινωνίας IoT

2.1 Περιγραφή και ορισμός του διαδικτύου των πραγμάτων IoT

Το IoT βασίζεται στην ενσωμάτωση ποικίλων διεργασιών όπως η ταυτοποίηση, η ανίχνευση, η δικτύωση και οι υπολογιστικές διεργασίες και καθιστά δυνατές τεχνολογικές καινοτομίες μεγάλης κλίμακας με υψηλές υπηρεσίες οι οποίες εξατομικεύουν την διάδραση του χρήστη με διάφορα <<πράγματα>>. [15] Μείζονος σημασίας για την αφετηρία IoT αποτελεί η ανταλλαγή δεδομένων από και προς τα διαδικτυωμένα αντικείμενα (Smart Things) με την ελάχιστη ανθρώπινη παρέμβαση. Τα συστήματα IoT σύμφωνα με την Melanie Swan (2012) έχουν πέντε βασικά λειτουργικά βήματα: τη δημιουργία δεδομένων, τη δημιουργία πληροφοριών, την αποσαφήνιση πληροφοριών και την εκτέλεση αποφάσεων.[7] Η ευρεία IP δικτύωση των ημερών μας (Internet), η εξέλιξη Analytics δεδομένων και του Cloud Computing διαδραμάτισαν καθοριστικό παράγοντα στην εξέλιξη της IoT τεχνολογίας.

Τα δεδομένα που συλλέγονται προέρχονται από διαδικτυωμένα ενσωματωμένα συστήματα που δίνουν πληροφόρηση για την συσκευή. Ως αποτέλεσμα αυτών των πληροφοριών εκτελούνται κάποιες αυτοματοποιημένες εργασίες. Τα δεδομένα των συσκευών προέρχονται από ενσωματωμένους αισθητήρες, οι οποίοι ανιχνεύουν φυσικά μεγέθη όπως η θερμοκρασία, η υγρασία, οι δονήσεις, ο ήχος, τα χημικά αέρια, η ροή υγρού, της πίεσης, του βάρους, της δύναμης, της στάθμης του υγρού, της επιτάχυνσης, της ταχύτητας, της κίνησης και της εγγύτητας.[8]



Εικόνα 2 Βασικοί τύποι αισθητηρίων [9]

Εκτός από τους αισθητήρες υπάρχουν και οι ενεργοποιητές, που όταν λαμβάνουν ένα σήμα, δρουν και ενεργοποιούνται. Με αυτόν τον τρόπο ξεκινάει μία εργασία είτε ηλεκτρική είτε μηχανική. Μέσω πολλών τύπων αισθητηρίων, τη συλλογή δεδομένων από αυτούς και το

συνδυασμό τους με ενεργοποιητές κατέστη δυνατό να γεφυρωθεί το χάσμα του φυσικού κόσμου με αυτόν του ψηφιακού.[8]

Μερικοί παρατηρητές βλέπουν το IoT ως επαναστατικό, ένα κόσμο προόδου, πλήρως διασυνδεδεμένο, αποτελεσματικό, δίνοντας ευκαιρία να προσθέσει δισεκατομμύρια αξίας στη βιομηχανία και στον κόσμο της οικονομίας. Άλλοι προειδοποιούν ότι το IoT αντιπροσωπεύει ένα σκοτεινότερο κόσμο με επιτήρηση της ιδιωτικότητας και της ασφάλειας των καταναλωτών.[10]

2.2 Όροι σύμφωνα με διεθνείς οργανισμούς

Στην παρούσα μεταπτυχιακή εργασία είναι χρήσιμο να αναφερθούν οι όροι από τους οργανισμούς και τους παρόχους που σχετίζονται με την ασφάλεια και τις τηλεπικοινωνίες

Σύμφωνα με τον οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών **Enisa** το Internet of Things (IoT) είναι μια αναδυόμενη ιδέα που περιγράφει ένα ευρύ οικοσύστημα όπου οι διασυνδεδεμένες συσκευές και υπηρεσίες συλλέγουν, ανταλλάσσουν και επεξεργάζονται δεδομένα προκειμένου να προσαρμοστούν δυναμικά σε ένα περιβάλλον. Το IoT συνδέεται στενά με τα cyber-physical systems και από αυτήν την άποψη με την χρήση των Έξυπνων Υποδομών βελτιώνεται η ποιότητα της παροχής υπηρεσιών. Η έξυπνη υποδομή, που υποστηρίζεται από τεχνολογίες όπως το IoT, προσφέρει πολλά πλεονεκτήματα με σημαντική εξοικονόμηση κόστους και αποτελεσματικότητα. Αυτά τα είδη περιβάλλοντος που βασίζονται σε δεδομένα, τροφοδοτούνται από συνδεδεμένες συσκευές και συνδεσιμότητα δικτύου, γίνονται μια νέα επιφάνεια επίθεσης για απειλές στον κυβερνοχώρο. Ο ENISA αναπτύσσει οδηγίες για την ασφάλεια των IoT και των έξυπνων υποδομών από απειλές στον κυβερνοχώρο, επισημαίνοντας καλές πρακτικές ασφάλειας και προτείνοντας συστάσεις σε φορείς εκμετάλλευσης, κατασκευαστές και υπευθύνους λήψης αποφάσεων. [16]

Για τον πολυεθνικό πάροχο κυβερνοασφάλειας και προστασίας από ιούς Kaspersky το Διαδίκτυο των πραγμάτων (IoT) είναι μια συλλογή συσκευών που είναι συνδεδεμένες στο Διαδίκτυο. Σκέφτεστε πιθανώς για πράγματα όπως ένα φορητό υπολογιστή ή μια έξυπνη τηλεόραση, αλλά το IoT περιλαμβάνει περισσότερα από αυτό. Σκεφτείτε ηλεκτρονικά που δεν ήταν ιστορικά συνδεδεμένα στο διαδίκτυο, όπως μηχανήματα φωτοτυπίας, ψυγεία στο σπίτι ή καφετιέρα στην αίθουσα αποσκευών. Το Διαδίκτυο των πραγμάτων αναφέρεται σε όλες τις συσκευές, ακόμη και σε εκείνες τις ασυνήθιστες συσκευές, που μπορούν να συνδεθούν στο Διαδίκτυο. Σχεδόν οτιδήποτε με διακόπτη

on / off αυτές τις μέρες μπορεί δυνητικά να συνδεθεί στο Διαδίκτυο, καθιστώντας το μέρος του IoT. Γιατί όλοι μιλούν για το IoT τώρα; Το IoT είναι ένα μείζον θέμα γιατί συνειδητοποιούμε πόσα πράγματα μπορούν να συνδεθούν και πώς μπορεί να επηρεάσει τις επιχειρήσεις.

Ένας συνδυασμός πραγμάτων καθιστά το IoT ώριμο για συζήτηση, όπως:

- Πιο προσιτοί τρόποι για τη δημιουργία συσκευών με γνώσεις τεχνολογίας
- Ένας αυξανόμενος αριθμός προϊόντων είναι συμβατά με Wi-Fi

- Η απότομη αύξηση της χρήσης smartphone
- Η δυνατότητα μετατροπής των smartphone σε ελεγκτές για άλλες συσκευές

- Για όλους αυτούς τους λόγους, το IoT δεν είναι πια απλή πληροφορική. Είναι ένας όρος που πρέπει να γνωρίζει κάθε ιδιοκτήτης επιχείρησης. [17]

Για τη Διεθνή ένωση Τηλεπικοινωνιών ITU το Διαδίκτυο των πραγμάτων (IoT) είναι μία παγκόσμια υποδομή για την κοινωνία της πληροφορίας, που επιτρέπει προηγμένες υπηρεσίες διασυνδέοντας (φυσικά και εικονικά) πράγματα με βάση τις υπάρχουσες και εξελισσόμενες διαλειτουργικές τεχνολογίες πληροφοριών και επικοινωνιών.

- Μέσω της αξιοποίησης της ταυτοποίησης, της συλλογής δεδομένων, της επεξεργασίας και της επικοινωνίας δυνατότητες, το IoT αξιοποιεί πλήρως τα πράγματα για να προσφέρει υπηρεσίες σε όλα τα είδη εφαρμογών, διασφαλίζοντας παράλληλα αυτό ενώ πληρούνται οι απαιτήσεις ασφάλειας και απορρήτου.
- Από μια ευρύτερη προοπτική, το IoT μπορεί να εκληφθεί ως ένα όραμα με τεχνολογικές και κοινωνικές επιπτώσεις.

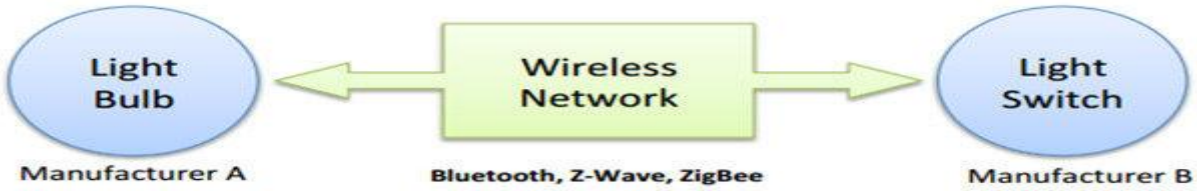
Όσον αφορά το Διαδίκτυο των πραγμάτων, αυτό είναι ένα αντικείμενο του φυσικού κόσμου (φυσικά πράγματα) ή τον κόσμο της πληροφορίας (εικονικά πράγματα), που μπορεί να ταυτοποιηθεί και να ενσωματωθεί σε δίκτυα επικοινωνίας. [18]

2.3 Μοντέλα επικοινωνίας IoT

Τον Μάρτιο του 2015, το Internet Architecture Board (IAB) κυκλοφόρησε ένα καθοδηγητικό αρχιτεκτονικό έγγραφο για τη δικτύωση έξυπνων αντικειμένων (RFC 7452). Αυτό περιγράφει τέσσερα κοινά μοντέλα επικοινωνίας όπως Device to Device, Device to Cloud, Device to Gateway και Back-End Sharing. [10]

2.3.1 Device-To-Device

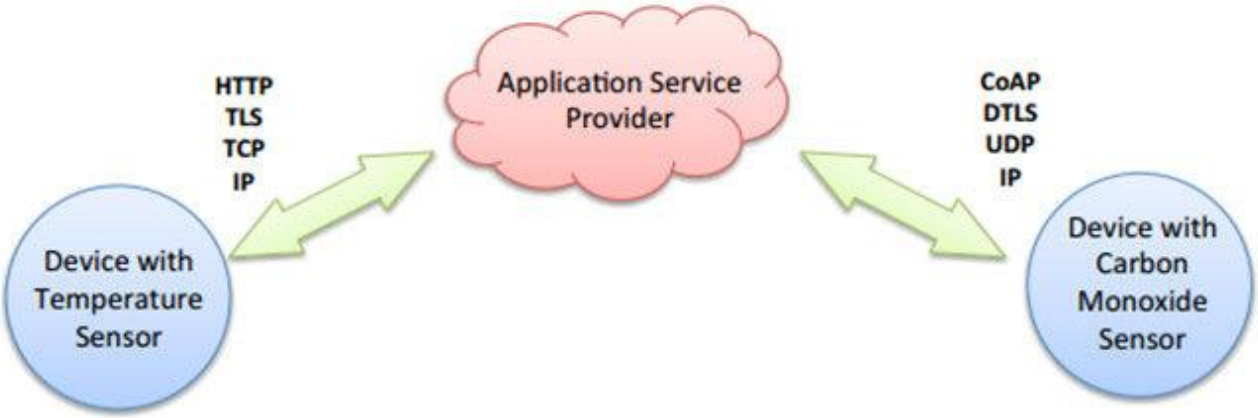
Το μοντέλο επικοινωνίας μεταξύ IoT συσκευών δύο ή και περισσότερων γίνεται εφικτό με την σύνδεσή τους, χωρίς να χρειάζεται απαραίτητα κάποια εφαρμογή για να καθορίζει την επικοινωνία των συσκευών. Η επικοινωνία Device-To-Device επιτυγχάνεται μέσω του διαδικτύου, του δικτύου IP, αλλά και με πρωτόκολλα επικοινωνίας όπως το Bluetooth, το RFID, το Z-WAVE και το ZigBee. Με το κατάλληλο πρωτόκολλο επικοινωνίας επιτυγχάνεται ανταλλαγή μηνυμάτων, ώστε οι συσκευές να εκτελούν αποδοτικά μεταξύ τους τις σχεδιαζόμενες λειτουργίες. Η χρήση αυτού του τρόπου επικοινωνίας χρησιμοποιεί μικρό ρυθμό δεδομένων και βρίσκει εφαρμογή σε μικρούς αυτοματισμούς όπως ο οικιακός. Επίσης θα πρέπει να δώσουμε έμφαση στην ιδιαίτερη δυσκολία διαλειτουργικότητας λόγω των διαφορετικών πρωτοκόλλων επικοινωνίας που χρησιμοποιούν οι συσκευές. Αυτό μπορεί να δημιουργήσει ασυμβατότητες μεταξύ τους και ο χρήστης να αναγκάζεται να επιλέγει ίδιας οικογένειας συσκευές από τον προμηθευτή. [10]



Εικόνα 3 Μοντέλο επικοινωνίας Device to Device [11]

2.3.2 Device-To-Cloud

Το μοντέλο επικοινωνίας μεταξύ συσκευής και σύννεφου (cloud) επιτυγχάνεται όταν η συσκευή IoT συνδέεται με τον πάροχο υπηρεσιών εφαρμογών για ανταλλαγή δεδομένων και έλεγχος κυκλοφορίας μηνυμάτων (Cloud) μέσω του Διαδικτύου με την Ethernet ή Wi-Fi δικτύωση του IoT. Η IoT συσκευή μεταδίδει δεδομένα σε μία Cloud βάση δεδομένων όπου τα δεδομένα μπορούν να χρησιμοποιηθούν για ανάλυση. Το Cloud επιτρέπει στον χρήστη από οποιαδήποτε τοποθεσία με σύνδεση στο διαδίκτυο να έχει απομακρυσμένη πρόσβαση με επέκταση των δυνατοτήτων της συσκευής. Θα πρέπει να δώσουμε έμφαση στην ιδιαίτερη πρόκληση διαλειτουργικότητας, καθώς πολλές συσκευές IoT προέρχονται από διαφορετικούς κατασκευαστές. [10]



Εικόνα 4 Μοντέλο επικοινωνίας Device to Cloud [12]

2.3.3 Device-to-Gateway

Οι πύλες δικτύου (Gateways IoT) διαδραματίζουν ένα κομβικό ρόλο στην IoT τεχνολογία, καθώς με την ραγδαία αύξηση έξυπνων συσκευών και την συνεχώς αυξητική τάση ετερογενών δεδομένων οι απαιτήσεις για πιο γρήγορη και αποτελεσματικότερη τεχνητή νοημοσύνη, για ασφάλεια και για ενσωμάτωση είναι επιβεβλημένη. Οι πύλες δικτύου συνδέουν τις συσκευές με το Cloud, όταν οι συσκευές δεν έχουν δυνατότητα απευθείας σύνδεσης στο διαδίκτυο μέσω του δρομολογητή, χρησιμοποιώντας τα πρωτόκολλα επικοινωνίας όπως το ZigBee (*εκτός του ZigBee 3.0*) και το Bluetooth. [10]

Οι πύλες IoT έχουν εξελιχθεί για την εκτέλεση πολλών εργασιών, από ένα απλό φιλτράρισμα δεδομένων έως τη δυνατότητα οπτικοποίησης, σύνθετων αναλυτικών στοιχείων, την τυποποίηση και τη μετάφραση πρωτοκόλλου IoT, τον έλεγχο συσκευής IoT, την κρυπτογράφηση δεδομένων IoT, τη συνάθροιση συνδεσιμότητας και την υποστήριξη υπολογιστικών ακρών (Edge computing). [19]

Μια ευέλικτη πύλη IoT μπορεί να εκτελέσει οποιοδήποτε από τα ακόλουθα [19] :

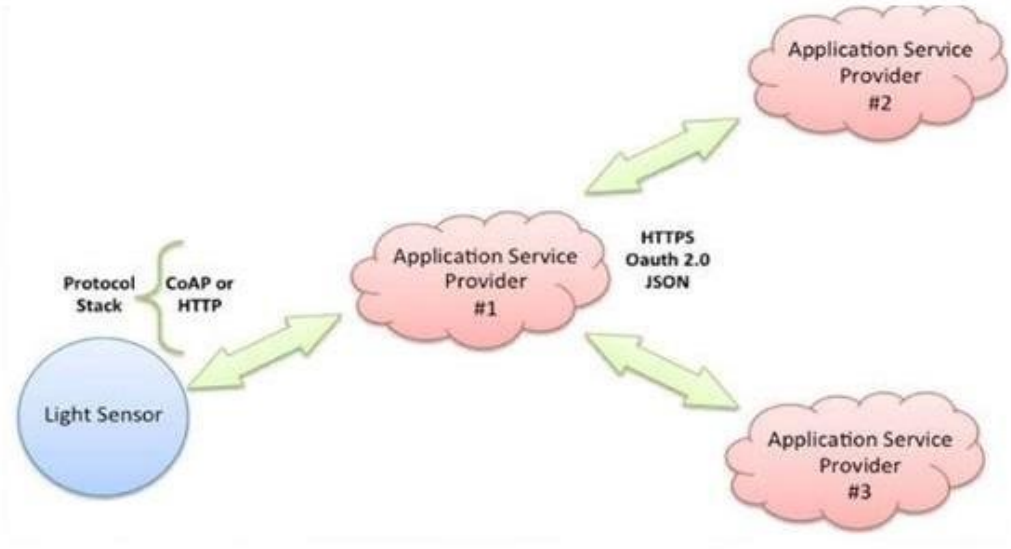
- Διευκόλυνση της επικοινωνίας με παλαιότερες ή συνδεδεμένες στο Διαδίκτυο συσκευές
- Προσωρινή αποθήκευση δεδομένων, προσωρινή αποθήκευση και ροή δεδομένων
- Προ επεξεργασία, καθαρισμός, φιλτράρισμα και βελτιστοποίηση δεδομένων
- Ορισμένες συγκεντρώσεις δεδομένων
- Επικοινωνία από συσκευή σε συσκευή
- Δυνατότητες δικτύωσης και φιλοξενία ζωντανών δεδομένων (live streaming)
- Οπτικοποίηση δεδομένων και βασική ανάλυση δεδομένων μέσω εφαρμογών IoT Gateway
- Βραχυπρόθεσμα χαρακτηριστικά ιστορικού δεδομένων
- Ασφάλεια πρόσβασης χρήστη και ασφάλεια δικτύου
- Διαχείριση διαμόρφωσης συσκευής
- Διαγνωστικά συστήματος

Εικόνα 5 Μοντέλο επικοινωνίας Device to Gateway [13]

2.3.4 Back-End Data-Sharing

Το μοντέλο Back-End Data-Sharing είναι μια αρχιτεκτονική επικοινωνίας, που επιτρέπει στους χρήστες να εξάγουν και να αναλύουν δεδομένα IoT συσκευών από μια cloud υπηρεσία σε συνδυασμό με δεδομένα από άλλες πηγές. Αποτελεί επέκταση του μοντέλου επικοινωνίας device to cloud, που επιτρέπει σε IoT συσκευές να ανεβάζουν δεδομένα μόνο για έναν πάροχο υπηρεσιών εφαρμογής. Μια αρχιτεκτονική back-end data-sharing επιτρέπει τη συγκέντρωση και ανάλυση των δεδομένων που συλλέγονται από τις ροές δεδομένων μιας συσκευής IoT.

Επίσης επιτρέπει σε τρίτους την πρόσβαση στα δεδομένα των αισθητήρων που έχουν μεταφορτωθεί στο cloud. [10]



Εικόνα 6 Μοντέλο επικοινωνίας Back End Data Sharing [14]

3 Τομείς Εφαρμογής IoT

Οι εφαρμογές του IoT είναι πολυάριθμες και ποικίλες, που καλύπτουν σχεδόν όλους τους τομείς τόσο σε καταναλωτικό όσο και σε επιχειρησιακό επίπεδο. Η λίστα που παρουσιάζεται παρακάτω, [20] περιλαμβάνει τα πιο μοντέρνα σενάρια εφαρμογών IoT και ομαδοποιείται σε δώδεκα διαφορετικούς τομείς, δείχνοντας πώς το διαδίκτυο των πραγμάτων γίνεται η επόμενη τεχνολογική επανάσταση.

3.1 Εφαρμογή IoT στις έξυπνες πόλεις

- Παρακολούθηση διαθεσιμότητας θέσεων στάθμευσης στην πόλη (Έξυπνος χώρος στάθμευσης).
- Παρακολούθηση των δονήσεων και την κατάσταση των υλικών στα κτίρια, γέφυρες και ιστορικά μνημεία (Κατάστασης υποδομών).
- Παρακολούθηση ήχου σε πραγματικό χρόνο σε κεντρικές ζώνες (Χαρτογράφηση ήχου πόλης).
- Παρακολούθηση οχημάτων και πεζών για βελτιστοποίηση σε διαδρομές οδήγησης και πεζοπορίας (Κυκλοφοριακή συμφόρηση).
- Προσαρμοσμένος στις καιρικές συνθήκες φωτισμός (Έξυπνος φωτισμός).
- Ανίχνευση των σκουπιδιών στα δοχεία για βελτιστοποίηση των διαδρομών των οχημάτων συλλογής απορριμμάτων (Διαχείριση αποβλήτων).
- Έξυπνοι δρόμοι και ευφυείς αυτοκινητόδρομοι με προειδοποιητικά μηνύματα και εκτροπές στην κυκλοφορία οχημάτων ανάλογα με τις κλιματικές συνθήκες και απρόσμενα γεγονότα όπως ατυχήματα ή μποτιλιαρίσματα (Ευφυή μέσα μαζικής μεταφοράς).

3.2 Εφαρμογή IoT στο Έξυπνο περιβάλλον

- Παρακολούθηση των αερίων καύσης και προληπτικών συνθηκών πυρκαγιάς για τον ορισμό ζωνών ειδοποίησης (Ανίχνευση πυρκαγιάς στο δάσος).
- Έλεγχος στις εκπομπές διοξειδίου του άνθρακα των εργοστασίων, την εκπεμπόμενη ρύπανση από αυτοκίνητα και τοξικά αέρια που παράγονται σε αγροκτήματα (Μέτρηση ατμοσφαιρικής ρύπανση).
- Μετρήσεις της υγρασίας του εδάφους, των δονήσεων και της πυκνότητα της γης για την ανίχνευση επικίνδυνων μοτίβων σε σχέση με τις συνθήκες του εδάφους (Πρόληψη κατολισθήσεων και χιονοστιβάδων).
- Κατανεμημένος έλεγχος σε συγκεκριμένα σημεία σεισμικών δονήσεων (Έγκαιρη ανίχνευση σεισμού).

3.3 Εφαρμογή IoT στο Έξυπνο νερό

- Μελέτη καταλληλόλητας του νερού σε ποτάμια και θάλασσα για την πανίδα και την επιλογή χρήση πόσιμου νερού (Ποιότητα νερού).
- Ανίχνευση νερού έξω από τις δεξαμενές και παρακολούθηση της διακύμανσης πίεσης κατά μήκος των σωλήνων (Διαρροές νερού).
- Παρακολούθηση των διακυμάνσεων της στάθμης του νερού σε ποτάμια, φράγματα και δεξαμενές (Πλημμύρες ποταμών).

3.4 Εφαρμογή IoT σε Smart Metering

- Συνεχή παρακολούθηση και διαχείριση κατανάλωσης ενέργειας (Smart Grid).
- Παρακολούθηση των επιπέδων νερού, πετρελαίου και φυσικού αερίου σε δεξαμενές αποθήκευσης και δεξαμενές (Επίπεδο δεξαμενής).
- Βελτιστοποίηση της απόδοσης ενέργειας με παρακολούθηση και διαχείριση φωτοβολταϊκών πάρκων (Φωτοβολταϊκές Εγκαταστάσεις).
- Μέτρηση της πίεσης του νερού σε συστήματα μεταφοράς του (Ροή νερού).
- Μέτρηση του κενού και του βάρους των εμπορευμάτων (Υπολογισμός αποθεμάτων).

3.5 Εφαρμογή IoT στην Ασφάλεια και Κρίσιμες Καταστάσεις

- Έλεγχος σε περιορισμένες περιοχές και ανίχνευση ατόμων σε μη εξουσιοδοτημένες περιοχές (Πρόσβαση περιμέτρου).
- Ανίχνευση σε υγρά στα κέντρα δεδομένων (Data Center), αποθήκες και σε κτίρια για την αποφυγή βραχυκυκλωμάτων και διάβρωσης (Έλεγχος διαρροής).
- Κατανεμημένη μέτρηση των επιπέδων ακτινοβολίας στην πυρηνική ενέργεια γύρω από τους σταθμούς για την ειδοποίηση διαρροής (Έλεγχος σε επίπεδα ακτινοβολίας).
- Ανίχνευση επιπέδων και διαρροών αερίου σε βιομηχανίες όπως χημικά εργοστάσια και στα ορυχεία (Έλεγχος εκρηκτικών και επικίνδυνων αερίων).

3.6 Εφαρμογή IoT στο Λιανεμπόριο

- Παρακολούθηση των συνθηκών αποθήκευσης κατά μήκος της αλυσίδας του εφοδιασμού και παρακολούθηση των προϊόντων με στόχο την ιχνηλασιμότητα (Έλεγχος της εφοδιαστικής αλυσίδας).
- Η επεξεργασία των πληρωμών γίνεται βάσει της τοποθεσίας ή της διάρκειας της εκάστοτε δραστηριότητας όπως σε δημόσιες συγκοινωνίες, γυμναστήρια και θεματικά πάρκα (Πληρωμή με NFC).
- Έξυπνες εφαρμογές αγορών: Λήψη συμβουλών στο σημείο πώλησης σύμφωνα με στις συνήθειες των πελατών, τις προτιμήσεις, την παρουσία αλλεργικών συστατικών για αυτούς ή ημερομηνίες λήξης.
- Έλεγχος της εναλλαγής προϊόντων σε ράφια και αποθήκες για την αυτοματοποίηση των διαδικασιών επανεκκίνησης (Έξυπνη διαχείριση προϊόντων).

3.7 Εφαρμογή IoT σε Logistics

- Παρακολούθηση των δονήσεων, των κτυπημάτων και των ανοιγμένων πακέτων για ασφαλιστικούς σκοπούς (Ποιότητα των συνθηκών αποστολής).
- Αναζήτηση μεμονωμένων αντικειμένων σε μεγάλες επιφάνειες όπως αποθήκες ή λιμάνια.
- Προειδοποίηση για αποθήκευση δοχείων με εύφλεκτα αγαθά κοντά σε άλλα που περιέχουν εκρηκτικά (Ανίχνευση ασυμβατότητας αποθήκευσης).
- Έλεγχος διαδρομών που ακολουθούνται για τα ευαίσθητα εμπορεύματα όπως τα φάρμακα, τα κοσμήματα και τα επικίνδυνα εμπορεύματα (Παρακολούθηση στόλου).

3.8 Εφαρμογή IoT στον Βιομηχανικό έλεγχο

- Αυτόματη διάγνωση μηχανής και έλεγχος στοιχείων ελέγχου (Εφαρμογές M2M).
- Παρακολούθηση των επιπέδων τοξικού αερίου και οξυγόνου εντός της χημικής ουσίας για την ασφάλεια των εργαζομένων και των εμπορευμάτων (Ποιότητα εσωτερικού αέρα).
- Έλεγχος θερμοκρασίας εντός βιομηχανικών και ιατρικών ψυγείων με ευαίσθητα εμπορεύματα (Παρακολούθηση θερμοκρασίας).
- Παρακολούθηση των επιπέδων του όζοντος κατά τη διαδικασία ξήρανσης του κρέατος σε εργοστάσια τροφίμων (Έλεγχος όζοντος).
- Στοιχεία της εσωτερικής τοποθεσίας χρησιμοποιώντας ενεργό (ZigBee) και παθητικές ετικέτες (RFID / NFC) (Εσωτερική τοποθεσία).
- Συλλογή πληροφοριών από CanBus για αποστολή σε πραγματικό χρόνο συναγερμών έκτακτης ανάγκης και προειδοποίηση των οδηγών (Αυτόματη διάγνωση οχήματος).

3.9 Εφαρμογή IoT στην Έξυπνη Γεωργία

- Παρακολούθηση της υγρασίας του εδάφους και της διαμέτρου των κορμών στους αμπελώνες γίνεται έλεγχος της περιεκτικότητας σε σάκχαρα στα σταφύλια και της υγείας των αμπελιών (Βελτίωση ποιότητας κρασιού).
- Έλεγχος των μικροκλιματικών συνθηκών για μεγιστοποίηση της παραγωγής φρούτων και λαχανικών και της ποιότητάς τους (Πράσινα σπίτια).

- Πρόβλεψη καιρικών αλλαγών όπως πάγου, βροχής, ξηρασίας, χιονιού και ανέμου (Δίκτυο μετεωρολογικών σταθμών).
- Έλεγχος των επιπέδων υγρασίας και θερμοκρασίας σε σανό, σε άχυρο για την αποφυγή μυκήτων και άλλων μικροβιακών ρύπων.

3.10 Εφαρμογή IoT στην Έξυπνη εκτροφή ζώων

- Έλεγχος στις συνθήκες των νέων ζώων στις κτηνοτροφικές μονάδες για την διασφάλιση της επιβίωσης και της υγείας τους (Φροντίδα Ζώων)
- Παρακολούθηση της θέσης και ταυτοποίηση των ζώων για τον τόπο που βόσκουν σε ανοιχτούς βοσκότοπους και την τοποθεσία τους σε μεγάλους στάβλους (Παρακολούθηση ζώων).
- Έλεγχος του εξαερισμού και της ποιότητα του αέρα σε αγροκτήματα και ανίχνευση των επιβλαβών αερίων (Επίπεδα τοξικού αερίου).

3.11 Εφαρμογή IoT στον Οικιακό αυτοματισμό

- Παρακολούθηση της κατανάλωσης ενέργειας και του νερού για να γίνεται εξοικονόμηση σε κόστος και σε πόρους (Χρήση ενέργειας και νερού).
- Ενεργοποίηση και απενεργοποίηση απομακρυσμένων συσκευών για πλήρη έλεγχο του χρήστη και εξοικονόμηση ενέργειας (Συσκευές τηλεχειρισμού).
- Ανίχνευση ανοιγμάτων παραθύρων και θυρών και παραβιάσεων για την αποτροπή εισβολέων (Συστήματα ανίχνευσης εισβολής).
- Παρακολούθηση των συνθηκών μέσα σε μουσεία και έργα τέχνης και αποθήκες (Διατήρηση τέχνης και αγαθών).

3.12 Ηλεκτρονική υγεία

- Βοήθεια σε ηλικιωμένους και σε άτομα με ειδικές ανάγκες που ζουν μόνοι τους (Ανίχνευση πτώσης).
- Έλεγχος συνθηκών μέσα σε καταψύκτες που αποθηκεύουν εμβόλια, φάρμακα και οργανικά στοιχεία (Ιατρικά ψυγεία).
- Παρακολούθηση ζωτικών σημάτων των αθλητών και επεξεργασία αυτών σε ψηφιακά κέντρα υψηλής απόδοσης (Φροντίδα αθλητών).
- Παρακολούθηση των συνθηκών για τους ασθενείς μέσα στα νοσοκομεία και στα γηροκομεία (Παρακολούθηση ασθενών).
- Μέτρηση της υπεριώδους ακτινοβολίας και προειδοποίηση με ηχητικά ή και με άλλα μέσα ώστε να μην εκτεθούν οι άνθρωποι σε αυτήν (Υπεριώδης ακτινοβολία).

4 Αναδυόμενες τεχνολογίες IoT

Λόγο του μεγάλου φάσματος εφαρμογών του IoT που έχουμε αναφέρει παραπάνω προκύπτουν νέες αναδυόμενες τεχνολογίες IoT. Αυτές θα διαδραματίσουν μεγάλο ρόλο στην πορεία των εξελίξεων IoT τεχνολογίας στους οργανισμούς, τις επιχειρήσεις, καθώς θα επηρεάσει την επιχειρηματική στρατηγική τους, αλλά και τους καταναλωτές. Ένα θέμα μείζονος σημασίας που θα κληθούν να αντιμετωπίσουν οι οργανισμοί είναι η διαχείριση κινδύνων, η αρχιτεκτονική και ο σχεδιασμός των δικτύων τους. Οι τεχνολογίες που αναδύονται θα ταξινομηθούν στους ακόλουθους δέκα τομείς. [21]

4.1 Ασφάλεια IoT

Στην σύγχρονη εποχή οι τεχνολογικές εξελίξεις παρουσιάζουν ταχύτατους ρυθμούς, η ασφάλεια καθιστά έναν σημαντικό παράγοντα για τις προκλήσεις που υπάρχουν. Λόγω του τεράστιου όγκου δεδομένων στο δίκτυο συνδεδεμένων «πραγμάτων» είναι απαραίτητη η ενίσχυση πολλαπλών επιπέδων ασφάλειας. Οι τεχνολογίες ασφάλειας καλούνται να προστατεύουν τις συσκευές, τις εφαρμογές και τις πλατφόρμες IoT τόσο από τις επιθέσεις πληροφοριών όσο και από τις φυσικές παραβιάσεις. Η ασφάλεια του IoT γίνεται ολοένα και πιο περίπλοκη, γιατί με την ραγδαία εξέλιξη της τεχνολογίας IoT πολλά "πράγματα" χρησιμοποιούν απλούς επεξεργαστές και λειτουργικά συστήματα που ενδέχεται να μην υποστηρίζουν εξελιγμένες προσεγγίσεις ασφάλειας. [21]

4.2 Εργαλεία ανάλυσης IoT και αλγόριθμοι

Τα επιχειρηματικά μοντέλα IoT εκμεταλλεύονται τις συλλεγόμενες πληροφορίες από τα IoT με πολλούς τρόπους. αυτοί θα απαιτήσουν νέα εργαλεία ανάλυσης και αλγόριθμους. Εφόσον οι όγκοι δεδομένων αυξάνονται εκθετικά ανά τα χρόνια, για τις ανάγκες του IoT γίνονται πολυσύνθετες και δεν καλύπτονται από τα παραδοσιακά εργαλεία ανάλυσης. [21]

4.3 Διαχείριση και παρακολούθηση συσκευών IoT

Τα IoT απαιτούν διαχείριση, παρακολούθηση, ενημέρωση υλικολογισμικού, λογισμικού, διαγνωστικά εργαλεία, ανάλυση σφαλμάτων και αναφορών, φυσική διαχείριση και διαχείρισης ασφάλειας συσκευών . Τα εργαλεία πρέπει να είναι ικανά να διαχειρίζονται και να παρακολουθούν χιλιάδες και ίσως ακόμη και εκατομμύρια συσκευές. [21]

4.4 Δίκτυα IoT χαμηλής ισχύος, μικρής εμβέλειας και μεσαίου εύρους

Τα ασύρματα μικρής εμβέλειας (Short range Wireless) λειτουργούν σε μη αδειοδοτημένες ζώνες συχνοτήτων γνωστές με τον όρο ISM. Τα περισσότερα ασύρματα πρότυπα μικρής εμβέλειας αποκαλούνται WPANs (Wireless Personal Area Networks) και έχουν εμβέλεια έως και 30 μέτρα. Όσα έχουν μεγαλύτερη εμβέλεια συχνά αποκαλούνται WLAN (Wireless Local Area Network). Παρακάτω παρουσιάζονται κάποια δίκτυα μικρής και μεσαίας εμβέλειας. [21]

4.4.1 Δίκτυα μικρής εμβέλειας

- Το πρωτόκολλο επικοινωνίας Bluetooth είναι γνωστό σε όλους μας από την εφαρμογή του στα κινητά τηλέφωνα και στα ασύρματα ακουστικά. Το Bluetooth λειτουργεί στην ζώνη ISM 2,4 GHz και είναι μια ανοιχτή ασύρματη τεχνολογία για το PAN. Τα κύρια πλεονεκτήματα στο πρωτόκολλο Bluetooth, χαμηλής ενέργειας (BLE) και Bluetooth Smart είναι ότι απαιτεί πολύ μικρή ισχύ από τη συσκευή και το κόστος του είναι πολύ χαμηλό. Η διασύνδεση που προσφέρει το Bluetooth είναι πολύ καθοριστική για την συλλογή δεδομένων σε IoT εφαρμογές.
- Η αναγνώριση ραδιοσυχνοτήτων RFID λειτουργεί μεταξύ των συχνοτήτων 135 KHz και των 5,875 GHz. Υπάρχουν ετικέτες RFID δύο ειδών οι ενεργές και οι παθητικές που επικοινωνούν με τους αναγνώστες RFID. Στις πρώτες εφαρμογές IoT που εφαρμόστηκε η αναγνώριση ραδιοσυχνοτήτων (RFID), ήταν αυτές για λύσεις εντοπισμού θέσης. Το μέλλον της τεχνολογίας RFID ξεπερνά σαφώς τις απλές υπηρεσίες εντοπισμού όπως την παρακολούθηση ασθενών σε νοσοκομεία, τη βελτίωση της αποτελεσματικότητας στην υγειονομική περίθαλψη και την παροχή δεδομένων τοποθεσίας σε πραγματικό χρόνο για τα εμπορεύματα για την βέλτιστη διαχείριση αποθεμάτων από τα καταστήματα λιανικής. [22]

4.4.2 Δίκτυα μεσαίας εμβέλειας IoT

- Το IEEE 802.11 -ευρέως γνωστό ως- Wi-Fi είναι το πιο διαδεδομένο και γνωστό πρωτόκολλο ασύρματων επικοινωνιών παγκοσμίως. Το Wi-Fi λειτουργεί στη ζώνη των συχνοτήτων 2,4GHz έως και 60GHz και υποστηρίζει ρυθμούς δεδομένων που κυμαίνονται από 1Mb/s έως 54Mb/s, αλλά επιταχύνει μέχρι και 6.75Gb/s. Η ευρεία χρήση του σε ολόκληρο τον κόσμο των IoT περιορίζεται από την υψηλή κατανάλωση ισχύος λόγω της ανάγκης για υψηλή ισχύ σήματος για την γρήγορη μεταφορά δεδομένων, για καλύτερη συνδεσιμότητα και για μεγαλύτερη αξιοπιστία.
- Το Zigbee είναι ένα δημοφιλές πρότυπο δικτύωσης ασύρματου πλέγματος, που βρίσκει τις πιο συχνές εφαρμογές του σε συστήματα διαχείρισης κυκλοφορίας, ηλεκτρονικά είδη οικιακής χρήσης και βιομηχανία μηχανών. Χτισμένο πάνω από το πρότυπο IEEE 802.15.4, το Zigbee υποστηρίζει χαμηλό ρυθμό ανταλλαγής δεδομένων, λειτουργία χαμηλής ισχύος, ασφάλεια και αξιοπιστία.
- Το Thread είναι σχεδιασμένο ειδικά για έξυπνα οικιακά προϊόντα. Χρησιμοποιεί συνδεσιμότητα IPv6 για να επιτρέπει σε συνδεδεμένες συσκευές να επικοινωνούν μεταξύ τους, να έχουν πρόσβαση σε υπηρεσίες στο cloud ή να αλληλοεπιδρούν με τον χρήστη μέσω εφαρμογών για κινητές συσκευές Thread. [22]

4.5 Δίκτυα IoT χαμηλής ισχύος, ευρείας περιοχής

Τα παραδοσιακά κυψελοειδή δίκτυα δεν παρέχουν καλό συνδυασμό τεχνικών χαρακτηριστικών και λειτουργικού κόστους για τις εφαρμογές IoT που χρειάζονται κάλυψη ευρείας περιοχής σε συνδυασμό με σχετικά χαμηλό εύρος ζώνης, καλή διάρκεια ζωής μπαταρίας, χαμηλό κόστος υλικού, λειτουργίας και υψηλή πυκνότητα σύνδεσης.

4.5.1 Δίκτυα ευρείας περιοχής

- Το NB-IoT είναι ένα προϊόν τεχνολογιών 3GPP, το Narrowband IoT είναι ένα ολοκαίνουργιο πρότυπο τεχνολογίας που εξασφαλίζει εξαιρετικά χαμηλή κατανάλωση ενέργειας. Χρησιμοποιεί την υπάρχουσα υποδομή δικτύου, η οποία διασφαλίζει όχι μόνο την παγκόσμια κάλυψη σε δίκτυα LTE, αλλά και την εγγυημένη ποιότητα σήματος. Σε πολλές περιπτώσεις, αυτό το γεγονός επιτρέπει την εφαρμογή NB-IoT αντί για λύσεις που απαιτούσαν την κατασκευή τοπικών δικτύων, όπως το LoRa ή το Sigfox.
- Το LTE-Cat M1 είναι ένα πρότυπο σύνδεσης χαμηλής ισχύος ευρείας περιοχής (LPWA) που συνδέει συσκευές IoT και M2M με απαιτήσεις μέσου ρυθμού δεδομένων. Υποστηρίζει μεγαλύτερους κύκλους ζωής της μπαταρίας και προσφέρει μεγαλύτερη κάλυψη σε σύγκριση με τις κυψελοειδείς τεχνολογίες όπως 2G, 3G ή LTE-Cat 1. Για να είναι συμβατό με το υπάρχον δίκτυο LTE, το CAT M1 δεν απαιτεί από τους παρόχους να δημιουργήσουν νέα υποδομή για να το εφαρμόσουν. Σε σύγκριση με το NB-IoT, το LTE Cat M1 αποδεικνύεται ιδανικό για περιπτώσεις χρήσης σε κινητά, καθώς ο χειρισμός του μεταξύ τοποθεσιών κυψέλης είναι σημαντικά καλύτερος και μοιάζει πολύ με το LTE υψηλής ταχύτητας.
- Το LoRaWAN είναι ένα πρωτόκολλο χαμηλής ισχύος Long Range Wide-Area Networking, που έχει βελτιστοποιηθεί για κατανάλωση χαμηλής ισχύος και υποστηρίζει μεγάλα δίκτυα με εκατομμύρια συσκευές. Στοχεύοντας σε εφαρμογές δικτύου ευρείας περιοχής (WAN), το LoRaWAN έχει σχεδιαστεί για να παρέχει WAN χαμηλής ισχύος με χαρακτηριστικά που απαιτούνται για την υποστήριξη χαμηλού κόστους, κινητής και ασφαλούς αμφίδρομης επικοινωνίας εντός IoT, M2M, έξυπνης πόλης και βιομηχανικών εφαρμογών.
- Το Sigfox παρέχει μια αποτελεσματική λύση συνδεσιμότητας για εφαρμογές M2M χαμηλής ισχύος που απαιτούν χαμηλά επίπεδα μεταφοράς δεδομένων, για τα οποία το εύρος Wi-Fi είναι πολύ μικρό, το εύρος κινητής τηλεφωνίας είναι πολύ ακριβό και έχει μεγαλύτερη κατανάλωση ενέργειας. Η Sigfox χρησιμοποιεί την UNB, μια τεχνολογία που της επιτρέπει να χειρίζεται χαμηλές ταχύτητες μεταφοράς δεδομένων από 10 έως 1.000 b/sec. Με κατανάλωση ενέργειας έως και 100 φορές λιγότερη σε σύγκριση με τις λύσεις κυψελοειδούς επικοινωνίας, παρέχει έναν τυπικό χρόνο αναμονής 20 ετών για μια μπαταρία 2.5Ah. Προσφέροντας ένα ισχυρό, ενεργειακά αποδοτικό και επεκτάσιμο δίκτυο ικανό να υποστηρίζει επικοινωνία μεταξύ χιλιάδων συσκευών που λειτουργούν με μπαταρία σε περιοχές αρκετών τετραγωνικών χιλιομέτρων, το Sigfox αποδεικνύεται κατάλληλο για διάφορες εφαρμογές M2M, όπως έξυπνο φωτισμό δρόμου, έξυπνους μετρητές, οθόνες ασθενών, ασφάλεια συσκευές και περιβαλλοντικούς αισθητήρες. [22]

4.6 Επεξεργαστές IoT

Οι επεξεργαστές και οι αρχιτεκτονικές που χρησιμοποιούνται από συσκευές IoT καθορίζουν πολλές από τις δυνατότητές τους, όπως εάν είναι ικανές για ισχυρή ασφάλεια και κρυπτογράφηση, κατανάλωση ενέργειας, εάν είναι αρκετά εξελιγμένοι για να υποστηρίξουν ένα λειτουργικό σύστημα, αναβαθμιζόμενο υλικολογισμικό και ενσωματωμένους παράγοντες διαχείρισης συσκευών. Η κατανόηση των επιπτώσεων των επιλογών επεξεργαστή θα απαιτήσει βαθιές τεχνικές δεξιότητες. [21]

4.7 Λειτουργικά συστήματα IoT

Τα παραδοσιακά λειτουργικά συστήματα όπως τα Windows και το iOS δεν έχουν σχεδιαστεί για εφαρμογές IoT. Καταναλώνουν υπερβολική ισχύ, χρειάζονται γρήγορους επεξεργαστές και σε ορισμένες περιπτώσεις δεν διαθέτουν χαρακτηριστικά, όπως εγγυημένη απόκριση σε πραγματικό χρόνο. Έχουν επίσης πολύ μεγάλο αποτύπωμα μνήμης για μικρές συσκευές και ενδέχεται να μην υποστηρίζουν τα μοντέλα που χρησιμοποιούν οι προγραμματιστές IoT. Κατά συνέπεια, έχει αναπτυχθεί ένα ευρύ φάσμα λειτουργικών συστημάτων ειδικά για το IoT που ταιριάζουν σε πολλά διαφορετικά αποτυπώματα υλικού και ανάγκες λειτουργιών. [21]

4.8 Επεξεργασία ροής συμβάντων

Ορισμένες εφαρμογές IoT θα παράγουν εξαιρετικά υψηλούς ρυθμούς δεδομένων που πρέπει να αναλυθούν σε πραγματικό χρόνο. Τα συστήματα που δημιουργούν δεκάδες χιλιάδες συμβάντα ανά δευτερόλεπτο είναι κοινά. Άλλα συστήματα δημιουργούν εκατομμύρια συμβάντα ανά δευτερόλεπτο ανά περίπτωση. Για την αντιμετώπιση τέτοιων απαιτήσεων, έχουν προκύψει πλατφόρμες κατανεμημένης ροής υπολογιστικής ισχύος, που μπορούν να επεξεργαστούν ροές δεδομένων με πολύ υψηλούς ρυθμούς και να εκτελούν εργασίες ανάλυσης δεδομένων σε πραγματικό χρόνο και αναγνώριση προτύπων. [21]

4.9 Πλατφόρμες IoT

Οι πλατφόρμες IoT συνδυάζουν πολλά από τα στοιχεία υποδομής ενός συστήματος IoT σε ένα μόνο προϊόν. Οι υπηρεσίες που παρέχονται από τέτοιες πλατφόρμες εμπίπτουν σε τρεις κύριες κατηγορίες: •

- Έλεγχος και λειτουργίες συσκευών χαμηλού επιπέδου, όπως οι επικοινωνίες, η παρακολούθηση και η διαχείριση συσκευών, η ασφάλεια και οι ενημερώσεις υλικολογισμικού.
- Απόκτηση, μετατροπή και διαχείριση δεδομένων IoT.
- Ανάπτυξη εφαρμογών IoT, που περιλαμβάνει λογική βάσει συμβάντων, προγραμματισμό εφαρμογών, οπτικοποίησης, αναλυτικά στοιχεία και προσαρμογή για σύνδεση σε εταιρικά συστήματα. [21]

4.10 Πρότυπα και οικοσυστήματα IoT

Τα πρότυπα και οι σχετικές διεπαφές προγραμματισμού εφαρμογών (API) είναι απαραίτητα, επειδή οι συσκευές IoT πρέπει να λειτουργούν και να επικοινωνούν. Επίσης λόγω του ότι πολλά επιχειρηματικά μοντέλα IoT βασίζονται στην κοινή χρήση δεδομένων μεταξύ πολλών συσκευών και οργανώσεων. [21] Στο άμεσο μέλλον οι απαιτήσεις αυτές θα έχουν αυξητική τάση.

5 Κυβερνοχώρος, απειλές και ασφάλεια IoT

Μια απειλή στον κυβερνοχώρο ή την ασφάλεια στον κυβερνοχώρο είναι μια κακόβουλη πράξη που επιδιώκει να καταστρέψει δεδομένα, να κλέψει δεδομένα και να διαταράξει ή να διακόψει την ψηφιακή ζωή γενικά. Οι απειλές στον κυβερνοχώρο περιλαμβάνουν ιούς υπολογιστών, παραβιάσεις δεδομένων, επιθέσεις άρνησης υπηρεσίας (DoS) και άλλους φορείς επίθεσης.
Οι απειλές στον κυβερνοχώρο αναφέρονται επίσης στην πιθανότητα επιτυχούς επίθεσης στον κυβερνοχώρο που στοχεύει στην απόκτηση μη εξουσιοδοτημένης πρόσβασης, ζημιάς, διακοπής ή κλοπής ενός περιουσιακού στοιχείου τεχνολογίας πληροφοριών, δικτύου υπολογιστών, πνευματικής ιδιοκτησίας ή οποιασδήποτε άλλης μορφής ευαίσθητων δεδομένων. Οι απειλές στον κυβερνοχώρο μπορούν να προέρχονται από έναν οργανισμό από αξιόπιστους χρήστες ή από απομακρυσμένες τοποθεσίες από άγνωστα μέρη.[24]

Εικόνα 7 Enisa, ETL 2020 (Enisa.europa.eu), Top Threats

5.1 Παράγοντες απειλών (Threat Agents)

Οι βασικοί παράγοντες απειλών (threat agents) συνοψίζονται στις κάτωθι κατηγορίες, για τις οποίες παρέχεται μια γενική διαβάθμιση αναφορικά με το επίπεδο δυσκολίας αναγνώρισης των επιθέσεων, του αντικτύπου τους και της πιθανότητας εκδήλωσής τους.[23]

5.1.1 Εχθρικά Έθνη-Κράτη

Τα εθνικά προγράμματα πολέμου στον κυβερνοχώρο παρέχουν αναδυόμενες απειλές στον κυβερνοχώρο που κυμαίνονται από προπαγάνδα, καταστροφή ιστοτόπων, κατασκοπεία, διακοπή βασικών υποδομών έως και καταστροφή αυτών. Τα προγράμματα που χρηματοδοτούνται από την κυβέρνηση είναι όλο και πιο εξελιγμένα και δημιουργούν προηγμένες απειλές σε σύγκριση με άλλους παράγοντες απειλής. Οι αναπτυσσόμενες δυνατότητές τους θα μπορούσαν να προκαλέσουν εκτεταμένες, μακροπρόθεσμες ζημίες στην εθνική ασφάλεια πολλών χωρών. Τα εχθρικά έθνη-κράτη ενέχουν τον υψηλότερο κίνδυνο λόγω της ικανότητάς τους να χρησιμοποιούν αποτελεσματικά τεχνολογία και εργαλεία ενάντια στους πιο δύσκολους στόχους, όπως διαβαθμισμένα δίκτυα και κρίσιμες υποδομές, όπως ηλεκτρικά δίκτυα και βαλβίδες ελέγχου αερίου.[24]

5.1.2 Τρομοκρατικές ομάδες

Οι τρομοκρατικές ομάδες χρησιμοποιούν όλο και περισσότερο τις κυβερνοεπιθέσεις για να βλάψουν τα εθνικά συμφέροντα. Είναι λιγότερο ανεπτυγμένες σε κυβερνοεπιθέσεις και έχουν μικρότερη τάση να επιδιώκουν κυβερνο-μέσα από τα εθνικά κράτη. Είναι πιθανό οι τρομοκρατικές ομάδες να παρουσιάσουν σημαντικές απειλές στον κυβερνοχώρο καθώς οι πιο τεχνικά ικανές γενιές εντάσσονται στις τάξεις τους.[24]

5.1.3 Εταιρικοί κατάσκοποι και οργανώσεις οργανωμένου εγκλήματος

Οι εταιρικοί κατάσκοποι και οι οργανώσεις οργανωμένου εγκλήματος ενέχουν κίνδυνο λόγω της ικανότητάς τους να πραγματοποιούν βιομηχανική κατασκοπεία για να κλέβουν εμπορικά μυστικά ή μεγάλης κλίμακας νομισματική κλοπή. Γενικά, αυτά τα μέρη ενδιαφέρονται για δραστηριότητες που βασίζονται στο κέρδος, είτε να αποκομίσουν κέρδος είτε να διαταράξουν την ικανότητα μιας επιχείρησης να αποκομίσει κέρδος επιτίθεται σε βασικές υποδομές ανταγωνιστών, κλέβουν εμπορικά μυστικά ή αποκτούν πρόσβαση και υλικό εκβιασμού.[24]

5.1.4 Hacktivists

Οι δραστηριότητες Hacktivists κυμαίνονται σε πολιτικά ιδανικά και ζητήματα. Οι περισσότερες hacktivist ομάδες ασχολούνται με τη διάδοση της προπαγάνδας αντί για την καταστροφή των υποδομών ή τη διακοπή των υπηρεσιών. Ο στόχος τους είναι να υποστηρίξουν την πολιτική ατζέντα τους και όχι να προκαλέσουν τη μέγιστη ζημιά σε έναν οργανισμό.[24]

5.1.5 Δυσαρεστημένοι εσωτερικοί

Οι δυσαρεστημένοι εμπιστευτικοί είναι μια κοινή πηγή εγκλήματος στον κυβερνοχώρο. Οι εσωτερικοί χρήστες συχνά δεν χρειάζονται υψηλό βαθμό γνώσης υπολογιστών για να εκθέσουν ευαίσθητα δεδομένα επειδή μπορεί να έχουν άδεια πρόσβασης στα δεδομένα. Οι απειλές του Insider περιλαμβάνουν επίσης τρίτους προμηθευτές και υπαλλήλους που ενδέχεται κατά λάθος να εισάγουν κακόβουλα προγράμματα σε συστήματα ή μπορεί να συνδεθούν σε έναν ασφαλή κάδο S3, να κατεβάσουν τα περιεχόμενά του και να το μοιραστούν στο διαδίκτυο με αποτέλεσμα παραβίαση δεδομένων. Ελέγξτε τα δικαιώματά σας S3 ή θα το κάνει κάποιος άλλος.[24]

5.1.6 Χάκερ

Οι κακόβουλοι εισβολείς θα μπορούσαν να εκμεταλλευτούν μια εκμετάλλευση μηδενικής ημέρας για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Οι χάκερ ενδέχεται να εισέλθουν σε συστήματα πληροφοριών για μια πρόκληση ή υπερηφάνεια. Στο παρελθόν, αυτό απαιτούσε υψηλό επίπεδο δεξιοτήτων. Σήμερα, αυτοματοποιημένα σενάρια επίθεσης και πρωτόκολλα μπορούν να ληφθούν από το Διαδίκτυο, καθιστώντας απλές τις εξελιγμένες επιθέσεις.[24]

5.1.7 Φυσικές καταστροφές

Οι φυσικές καταστροφές αποτελούν απειλή στον κυβερνοχώρο, επειδή μπορούν να διαταράξουν την βασική σας υποδομή, όπως θα μπορούσε να κάνει μια επίθεση στον κυβερνοχώρο.[24]

5.1.8 Τυχαίες ενέργειες εξουσιοδοτημένων χρηστών

Ένας εξουσιοδοτημένος χρήστης μπορεί να ξεχάσει να ρυθμίσει σωστά την ασφάλεια S3, προκαλώντας πιθανή διαρροή δεδομένων. Ορισμένες από τις μεγαλύτερες παραβιάσεις δεδομένων οφείλονται σε κακή διαμόρφωση και όχι σε χάκερ ή σε δυσαρεστημένους εσωτερικούς.[24]

5.2 Ένα μεταβαλλόμενο περιβάλλον απειλών

Οι τεχνολογικές εξελίξεις, η ψηφιακή διακυβέρνηση αλλά και η ευημερία των χωρών μελών της Ευρωπαϊκής Ένωσης, έχουν καταστήσει τα κράτη-μέλη στόχους πληθώρας κυβερνοεπιθέσεων. Από απειλές που προέρχονται από μεμονωμένους εγκληματίες , μέχρι επιθέσεις φερόμενες ως απόρροια ενεργειών τρίτων κρατών, το περιβάλλον κυβερνοαπειλών είναι διαρκώς μεταβαλλόμενο, οδηγώντας σε μια εγγενή αδυναμία άμεσης προστασίας του. Οι εν λόγω συνθήκες επιβεβαιώνουν την ανάγκη για μια περιοδικά αναθεωρούμενη στρατηγική, η

οποία θα θέτει τους κανόνες αντιμετώπισης ή μετριασμού του αντίκτυπου των εν λόγω απειλών.[24][23]

5.2.1 Κακόβουλο λογισμικό (malicious software)

Λογισμικό το οποίο έχει σχεδιαστεί ειδικά για να προκαλέσει ζημιά ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή. Περιλαμβάνει ιούς(viruses), worms, trojan horses κ.λπ. Σε αυτή την κατηγορία ανήκει και το λογισμικό λύτρων (ransomware), το οποίο όμως εξετάζεται χωριστά λόγω της ιδιαιτερότητάς του.[23][25]

5.2.2 Επιθέσεις από το διαδίκτυο (web based attacks)

Πρόκειται για απειλές που στοχεύουν απευθείας στο χρήστη μέσω εκμετάλλευσης αδυναμιών στους φυλλομετρητές (browsers), καθώς και στα συστήματα διαχείρισης περιεχομένου (content management systems). Κυριότερα είδη επιθέσεων αυτής της κατηγορίας αποτελούν τα browser exploits, drive-by downolads, watering hole attacks κ.α.[23][25]

5.2.3 Phishing

Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές συνδιαλλαγές, οι οποίες αποσκοπούν στο να παραπλανήσουν τους χρήστες και να αποκαλύψουν εμπιστευτικές πληροφορίες.[23][25]

5.2.4 Επιθέσεις σε διαδικτυακές εφαρμογές (web application attacks)

Επιθέσεις που στοχεύουν σε διαδικτυακές εφαρμογές (web applications). Οι εν λόγω εφαρμογές λόγω της καθολικής χρήσης τους στην προσφορά περιεχομένου αποτελούν στόχο πολλαπλών ειδών επιθέσεων, με κυριότερες τα cross-site scripting (XSS), SQL injection, path traversal, local file inclusion κ.α.[23][25]

5.2.5 Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου

Αναφερόμενες και ως SPAM, αυτές οι επιθέσεις περιλαμβάνουν την αποστολή ανεπιθύμητης αλληλογραφίας σε χρήστες. Η εν λόγω αλληλογραφία χαρακτηρίζεται από το πολύ μικρό κόστος αποστολής των μηνυμάτων, την ενόχληση που προκαλεί στους χρήστες, αλλά και την εν δυνάμει μετεξέλιξη των μηνυμάτων σε απειλή phishing.[23][25]

5.2.6 Επιθέσεις άρνησης υπηρεσίας (Denial of Service – DoS attacks)

Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα.

Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας).[23][25]

5.2.7 Κλοπή ταυτότητας χρήστη (identity theft)

Ο επιτιθέμενος αποκτά δεδομένα προσωπικού χαρακτήρα του χρήστη (passwords, social security numbers κ.α.), με αποτέλεσμα την ιδιοποίηση της ταυτότητας του χρήστη (impersonation) και με σκοπό το οικονομικό όφελος (αγορές προϊόντων μέσω πιστωτικών καρτών, παράνομη επιστροφή φόρου κ.λπ.) εις βάρος του.[23][25]

5.2.8 Παραβιάσεις προσωπικών δεδομένων

Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679, τέτοιου είδους επιθέσεις νοούνται ως παραβιάσεις δεδομένων προσωπικού χαρακτήρα οι οποίες χρήζουν άμεσης αντιμετώπισης.[23][25]

5.2.9 Εσωτερικές απειλές (insider threat)

Απειλές που προέρχονται από στελέχη Φορέων που εργάζονται ή εργάζονταν σε έναν Οργανισμό, καθώς και εξωτερικών συνεργατών, οι οποίοι κατέχουν εσωτερική πληροφόρηση σχετικά με τις πρακτικές ασφάλειας, τα υπολογιστικά συστήματα και τα δεδομένα του Οργανισμού. Οι εν λόγω απειλές μπορούν να οδηγήσουν σε πλήθος επιθέσεων που περιγράφονται στην παρούσα ενότητα, συνήθως με πολύ μεγάλο αντίκτυπο για τον Φορέα και είναι εξαιρετικά δύσκολο να διαγνωσθούν ή/και αντιμετωπισθούν.[23][25]

5.2.10 Botnets

Δίκτυα τα οποία αποτελούνται από υπολογιστικές συσκευές ανυποψίαστων χρηστών που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται κεντρικά από κάποιον επιτιθέμενο, προκειμένου να χρησιμοποιηθούν ομαδικά στην αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας, σε επιθέσεις άρνησης υπηρεσίας, σε cryptojacking, κλπ.[23][25]

5.2.11 Φυσικές απειλές

Απειλές που στοχεύουν στην καταστροφή ή αλλοίωση ή κλοπή εξοπλισμού, με απώτερο στόχο την διαρροή ή/και καταστροφή δεδομένων ή την άρνηση υπηρεσίας.[23][25]

5.2.12 Διαρροή δεδομένων

Διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες. Τα δεδομένα μπορεί να περιλαμβάνουν οικονομικά στοιχεία, πατέντες, δεδομένα με κατοχυρωμένα πνευματικά δικαιώματα, πλάνα στρατηγικής ανάπτυξης κλπ.[23][25]

5.2.13 Λογισμικό λύτρων (ransomware)

Κακόβουλο λογισμικό (malware) το οποίο κρυπτογραφεί τα δεδομένα του πληροφοριακού συστήματος, για την αποκρυπτογράφηση των οποίων ο επιτιθέμενος απαιτεί λύτρα (συνήθως σε μορφή κρυπτονομίσματος).[23][25]

5.2.14 Ηλεκτρονική κατασκοπία

Κατασκοπία μέσω του κυβερνοχώρου, η οποία μπορεί να περιλαμβάνει χρήση εξειδικευμένων εργαλείων για την άντληση στοιχείων ή/και χρήση συνδυασμού των προαναφερθέντων απειλών. Συνήθως αυτή η μορφή επίθεσης αναφέρεται ως «στοχευμένη» (λόγω του ότι οι επιτιθέμενοι έχουν πολύ συγκεκριμένους στόχους) με απώτερο στόχο την υποκλοπή ευαίσθητων, για τον οργανισμό, πληροφοριών.[23][25]

5.2.15 Cryptojacking

Τεχνικές που χρησιμοποιούν την υπολογιστική ισχύ του υπολογιστή του χρήστη με σκοπό την άντληση (mining) κρυπτονομισμάτων (bitcoins).[23][25]

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking:** ↗ Going up, --- Same, ↙ Going down

Εικόνα 8 Οι 15 κορυφαίες απειλές σύμφωνα με τον Enisa [25]

6 Κατευθυντήριες γραμμές για την διασφάλιση της ασφάλειας σε IoT

6.1 Αλυσίδα εφοδιασμού IoT συσκευής

Η αλυσίδα εφοδιασμού για IoT αποτελείται από δύο κατηγορίες: τη φυσική και τη λογική.
Η φυσική αλυσίδα εφοδιασμού σχετίζεται με όλα τα αντικείμενα όπως: οι συσκευές, τα ηλεκτρονικά εξαρτήματα, και όλες τις χειροκίνητες διαδικασίες της συναρμολόγησης και της διανομής.
Η λογική αλυσίδα εφοδιασμού σχετίζεται με την ανάπτυξη λογισμικού, τις επικοινωνίες με βάση το δίκτυο και τις εικονικές αλληλεπιδράσεις μεταξύ των αντικειμένων IoT και των τελικών χρηστών.

Οι κίνδυνοι της αλυσίδας εφοδιασμού IoT σχετίζονται με τον τρόπο ανάπτυξης και της ολοκλήρωσης της τεχνολογίας που θα χρησιμοποιηθεί στο προϊόν έως και την αναβάθμιση του για την επίλυση δυσλειτουργιών που μπορεί να είναι και κενά ασφαλείας. [26]

6.2 Σύλληψη ιδέας σχεδιασμός IoT συσκευής

Κατά τη σύλληψη της ιδέας και του σχεδιασμού IoT συσκευής τα προϊόντα και οι υπηρεσίες έχουν σχεδιαστεί όπως λογισμικό και υλικό καθώς και άλλες υπηρεσίες που ενδέχεται να εμπλέκονται βρίσκονται σε επίπεδο εννοιολογικό. Αυτό το πρώιμο στάδιο είναι σημαντικό για να καθοριστούν τα βασικά θεμέλια ασφάλειας που θα αποτελούν μέρος των απαιτήσεων κατά τα επόμενα στάδια της αλυσίδας του εφοδιασμού. Η ασφάλεια στη φάση σχεδιασμού είναι κρίσιμη, καθώς ορισμένες αποφάσεις ή λάθη που βασίζονται στο κόστος σε αυτό το στάδιο μπορεί να οδηγήσουν σε ατέλειες ασφαλείας στο τελικό προϊόν.
Αυτή η φάση περιέχει το σχεδιασμό μοντέλων ασφαλείας στην αλυσίδα εφοδιασμού είτε στο Hardware είτε στο Software για την συνύπαρξη τόσο της φυσικής ασφάλειας όσο και της ψηφιακής ασφάλειας. [26]

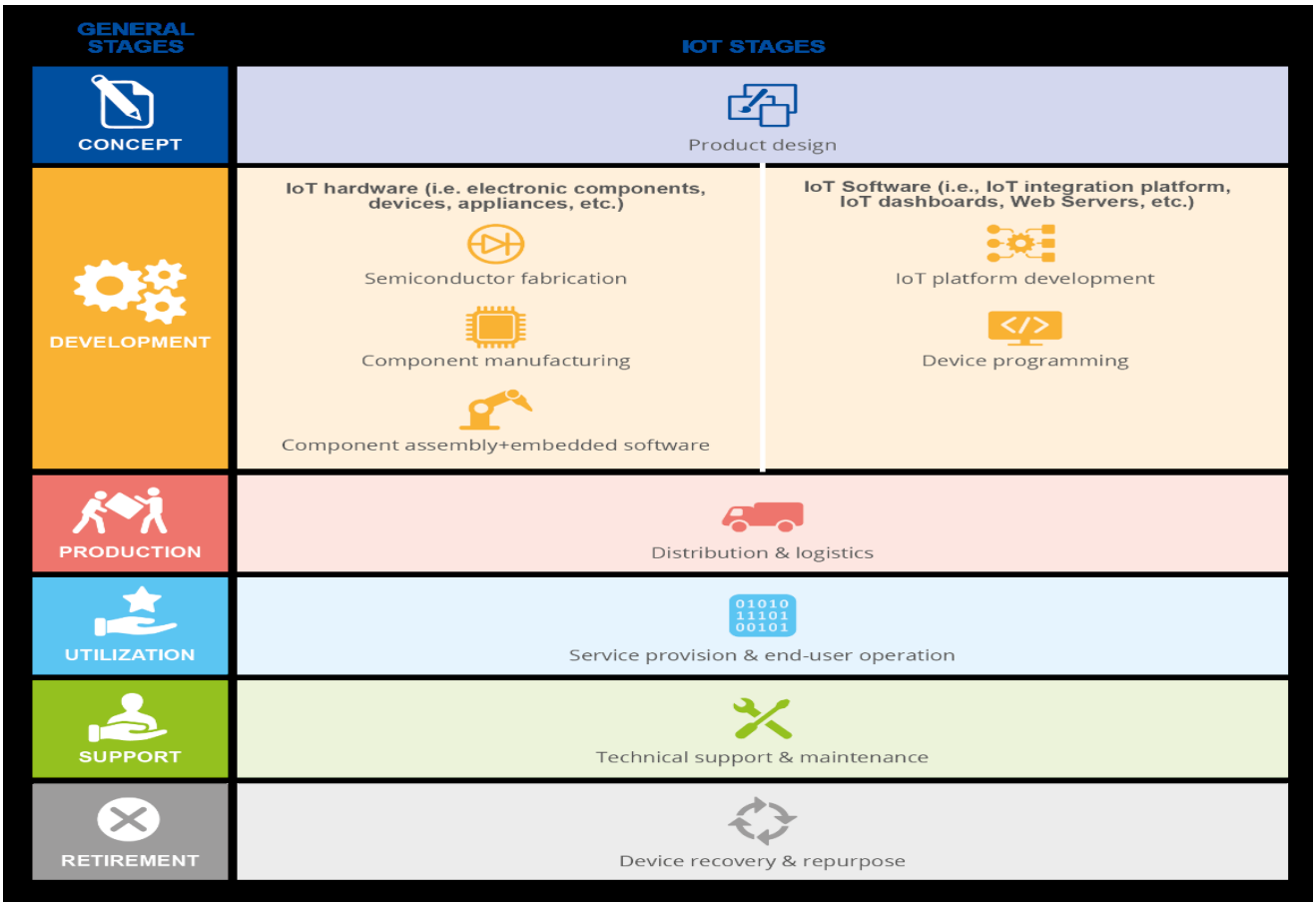
6.3 Ανάπτυξη IoT συσκευής

Οι εργασίες για την ανάπτυξη της συσκευής στην εκτείνονται από την κατασκευή ημιαγωγών έως τον προγραμματισμό υλικολογισμικού ώστε να φτάσουμε σε σημείο παραγωγής της συσκευής έτοιμη για αποστολή στους πελάτες. Σε αυτή την φάση περιλαμβάνεται η ανάπτυξη υπηρεσιών λογισμικού και κάποιες πλατφόρμες που απαιτούνται για τη λειτουργία και την ανάπτυξη συσκευών IoT Σ επίπεδο ασφαλείας αυτή είναι μια από τις πιο κρίσιμες φάσεις, καθώς οι περισσότεροι κίνδυνοι και απειλές προκύπτουν από κακές αποφάσεις, παραλείψεις ή λάθη σε αυτό το σημείο.
Μία τυπική συσκευή IoT θα περάσει από πολλά βήματα κατά τη φάση ανάπτυξης. Αυτά τα βήματα μπορούν να ταξινομηθούν κατά προσέγγιση στο Hardware και στο Software. Το Hardware περιλαμβάνει στοιχεία στην κατασκευή ημιαγωγών σύμφωνα με τις οδηγίες σχεδιασμού, στην κατασκευή PCB, στην ενσωμάτωση εξαρτημάτων και στη λειτουργική δοκιμή. Το Software περιλαμβάνει στοιχεία όπως τα on-chip microcode, τα λειτουργικά συστήματα, το middleware, τις βιβλιοθήκες τρίτων, την ενσωμάτωση υπηρεσιών την υπηρεσία σύννεφου (cloud) και διάφορα εργαλεία ανάπτυξης. [26]

6.4 Παραγωγή IoT συσκευής

Ένα σημαντικό ποσοστό των συσκευών IoT χρησιμοποιούν πολλές μονάδες από διαφορετικούς προμηθευτές και συνεπώς απαιτούν μια ευρεία, και συχνά περίπλοκη, αλυσίδα εφοδιασμού. Αυτό συνήθως οδηγεί σε μια πολύπλευρη λογική πρόκληση, όπου η παρακολούθηση όλων των σταδίων και των πηγών δεν είναι εύκολη υπόθεση.
Η μαζική παραγωγή, διανομή και εφοδιαστική έχει σχέση με τμήμα υποστήριξης και απόσυρσης, καθώς οι προκλήσεις που εμπλέκονται στην αρχική διανομή επανεμφανίζονται όταν τα προϊόντα πρέπει να ανακτηθούν λόγω δυσλειτουργίας ή να απορριφθούν.

Η παραγωγή της αλυσίδας εφοδιασμού IoT μπορεί να οριστεί ως η προσπάθεια που απαιτείται για την αποτελεσματική και ασφαλή παράδοση παρακολουθώντας όλες τις μονάδες σε συσκευές IoT. Συνήθως, αυτό περιλαμβάνει πολλούς διαφορετικούς παράγοντες: ναυτιλία, αποθήκευση, διαχείριση αποθεμάτων, λειτουργία στόλου παράδοσης, συσκευασία, χειρισμός και την υποστήριξη πελατών. [26]



Εικόνα 9 Αλυσίδα εφοδιασμού IoT [26]

6.5 Χρησιμοποίηση IoT συσκευής

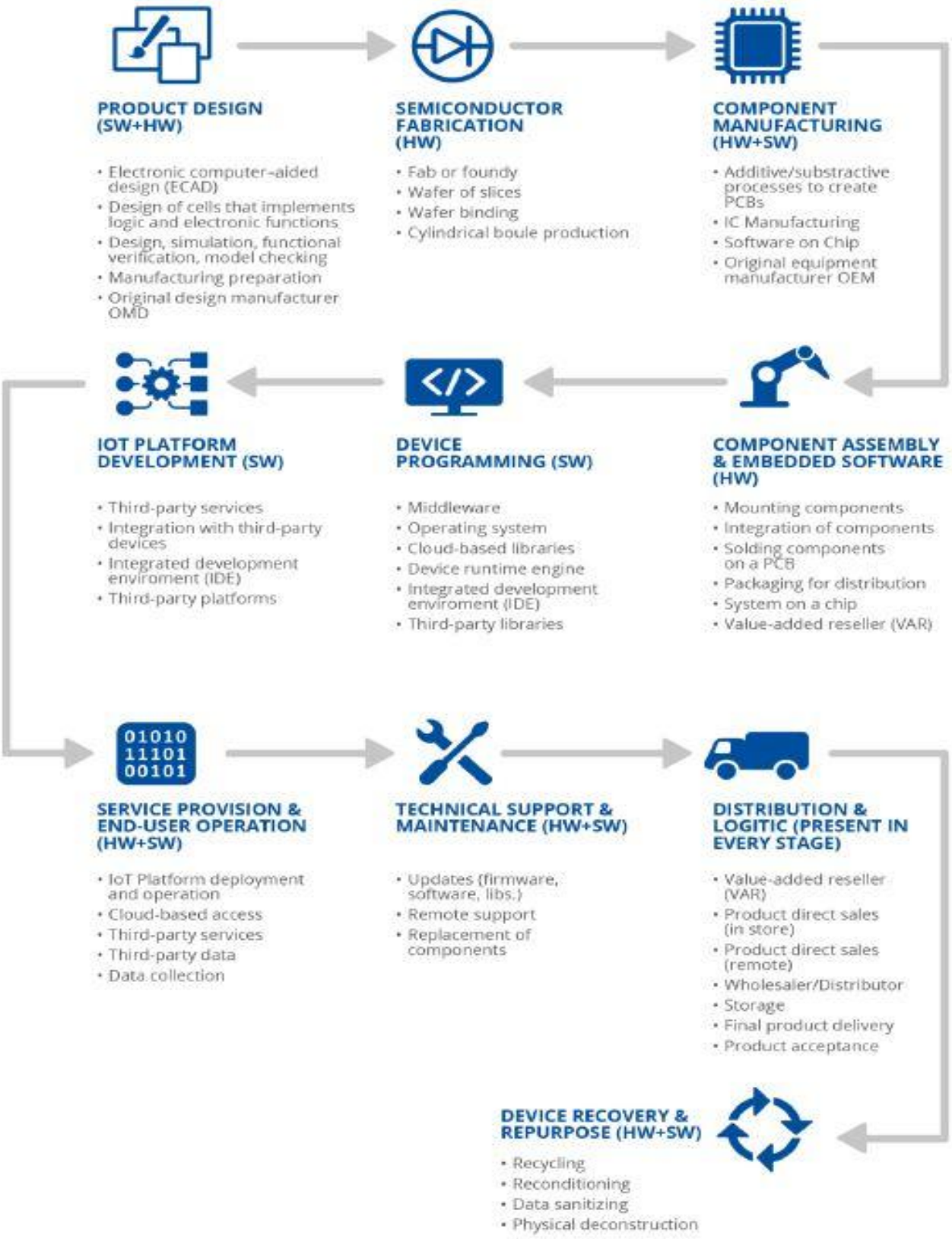
Η ενεργοποίηση και η λειτουργία της συσκευής στην τελική τοποθεσία του πελάτη εξαρτάται σε μεγάλο βαθμό από τον τύπο της συσκευής και τις παρεχόμενες υπηρεσίες.
Για μια τυπική συσκευή, αυτό συνήθως περιλαμβάνει εργασίες όπως: την παράδοση στον πελάτη ή τους εμπόρους λιανικής, την φυσική εγκατάσταση στη θέση λειτουργίας, την αρχική ρύθμιση της συσκευής, την δημιουργία ασφαλών διαπιστευτηρίων χρήστη τόσο σε επίπεδο συσκευής όσο και σε απομακρυσμένες υπηρεσίες, την σύζευξη με κινητές συσκευές και τις υπηρεσίες cloud για την συλλογή, την κοινή χρήση και την επεξεργασία δεδομένων. [26]

6.6 Υποστήριξη IoT συσκευής

Όταν σκεφτόμαστε τη φάση υποστήριξης στον κύκλο ζωής ενός προϊόντος, τείνουμε πάντα να σκεφτόμαστε για την αποκατάσταση ζημιών ή την επίλυση προβλημάτων. Από την προοπτική της αλυσίδας εφοδιασμού σε συσκευές IoT αυτό σημαίνει συχνά επισκευή ή αντικατάσταση κατεστραμμένων μονάδων. Οι συσκευές IoT είναι πολύ επιρρεπείς σε ζημιές και δυσλειτουργίες, καθώς οι προμηθευτές IoT έχουν συνήθως καλή ομάδα εργασίας ως υποστήριξη του προϊόντος τους, που συνεργάζονται στενά με τους προγραμματιστές και τους χρήστες, εάν χρειάζεται.
Αλλά υπάρχει ένα άλλο πολύ σημαντικό μέρος της φάσης υποστήριξης που περιστρέφεται γύρω από τη συνεχή επίβλεψη της ασφάλειας της μονάδας. Αυτό το μέρος διαιρείται κυρίως μεταξύ της διατήρησης ενημερώσεων για τις συσκευές (υλικολογισμικό, λογισμικό και βιβλιοθήκες) και απομακρυσμένη υποστήριξη.
Για αυτήν τη φάση της αλυσίδας εφοδιασμού, η έκθεση επικεντρώνεται στην πτυχή της συνεχούς πρόληψης. Η πλειονότητα των συσκευών IoT είναι ευρέως διαδεδομένες και συνήθως έχουν διάφορα συστατικά με διαφορετική προέλευση. Αυτό καθιστά ακόμη πιο δύσκολο να διασφαλιστεί η ασφάλεια των συσκευών και ακόμη και απειλές για τη λειτουργικότητα του προϊόντος. Αυτός είναι ο λόγος που πολλά μέτρα ασφαλείας και καλές πρακτικές έχουν επικεντρωθεί σε αυτήν τη φάση, χρησιμοποιώντας διαφορετικές τεχνολογίες και πρότυπα για να διασφαλιστεί η σωστή υποστήριξη των συσκευών IoT μέσω του κύκλου ζωής του. [26]

6.7 Απόσυρση IoT συσκευής

Για να έχουμε μια ασφαλή απόσυρση σε συσκευές IoT πρέπει να διασφαλιστεί μια σειρά βημάτων. Μία από τις βασικές πτυχές αυτής της φάσης είναι η ασφαλής αφαίρεση των πληροφοριών στη συσκευή IoT.
Εάν χρειαστεί, ένα άλλο βήμα στη διάθεση μιας συσκευής είναι η φυσική καταστροφή της. Αυτό παρουσιάζει προκλήσεις όχι μόνο στο τμήμα ασφάλειας στον κυβερνοχώρο, αλλά και στον τομέα της εφοδιαστικής και του περιβάλλοντος, καθώς τα απόβλητα ηλεκτρονικών συσκευών συνεπάγονται με πολλά προβλήματα μόλυνσης. Ένα από αυτά τα προβλήματα είναι η έλλειψη ορισμένων υλικών που χρησιμοποιούνται για τη δημιουργία τους, επομένως ένα σημαντικό μέρος της διαδικασίας απόσυρσης είναι η ανακύκλωση των συσκευών.
Έτσι, η διαδικασία απόσυρσης μπορεί να συνοψιστεί ως η ανακύκλωση των συσκευών με οικονομικά εφικτούς και φιλικούς προς το περιβάλλον τρόπους, τηρώντας παράλληλα τα πρότυπα ασφάλειας και απορρήτου. [26]



Εικόνα 10 Χάρτης αλυσίδας εφοδιασμού IoT [26]

7 Απειλές στην αλυσίδα εφοδιασμού IoT

Οι απειλές που αφορούν την αλυσίδα ανεφοδιασμού ταξινομούνται σε κατηγορίες υψηλού επιπέδου. Όλες οι απειλές περιλαμβάνουν μια σύντομη περιγραφή και το επίπεδο των σταδίων της εφοδιαστικής λίστας της αλυσίδας IoT που πιθανότατα επηρεάζουν. Αυτό δεν σημαίνει ότι άλλα στάδια δεν σχετίζονται με μια απειλή, αλλά τα στάδια που επηρεάζονται είναι οι φάσεις στις οποίες οι απειλές είναι πιο επικίνδυνες και μπορούν να αντιμετωπιστούν πιο αποτελεσματικά. [26]

7.1 Φυσικές επιθέσεις

Κατά την παραγωγή και συναρμολόγηση της IoT συσκευής κάποιος κακόβουλος παράγοντας έχει την ευκαιρία να παρέμβει στην συσκευή και να της δημιουργήσει ελαττώματα, δυσλειτουργίας ή και καταστροφή της συσκευής σε μεταγενέστερα στάδια. Η απειλή επίθεσης σε διαδικασίες παραγωγής είναι σχετική και σχετίζεται στενά στο πλαίσιο της σαμποτάζ.Τα προϊόντα ενδέχεται να διοχετευτούν σε μη εξουσιοδοτημένους διανομείς με αποτέλεσμα ελαττωματικά, απορριφθέντα ή χαμένα προϊόντα να καταλήγουν σε κακόβουλους παράγοντες. Η κατάληξη αυτή θα έχει απρόβλεπτες συνέπειες και δυσκολίες στην εφαρμογή αυστηρών προτύπων ασφάλειας και ποιότητας, συνεπώς τα προϊόντα θεωρούνται αναξιόπιστα. [26]

Sabotage	
The assembly pipeline may provide malicious actors with the opportunity to interfere and inject defects that may end up causing problems (up to the total shutdown and malfunction of the product) in later stages. The threat of attacking manufacturing processes (independently discussed in another category) is relevant and closely related in the context of sabotage.	• Component assembly & embedded software.

Grey markets	
Defective, discarded or lost products may end up in grey markets that exist outside of the proper distribution channels. This can lead to unforeseen consequences and add numerous difficulties to the implementation of strict security and quality standards by injecting untested and unreliable products into the market.	• Technical support & maintenance. • Device disposal & decommissioning.

Exploitation of inadequate physical enclosures	
Some devices require to be physically tamper-proof depending on the scenario. The choice of materials and construction method must be adequate for the intended use of the product. For instance, it doesn't matter how good the software of a smart lock is if the device can be easily torn apart with bare hands . Besides worrying about the physical enclosure, the designer should also consider how ports are included in the case. For instance, a maintenance port only used in manufacturing can be used by an attacker in the field. This port should be disabled or removed prior to field installation.	• Service provision & end-user operation. • Technical support & maintenance.

Εικόνα 11 Φυσικές επιθέσεις [26]

7.2 Επιθέσεις ενάντια στη πνευματική ιδιοκτησία

Οι κακόβουλοι παράγοντες εκμεταλλεύονται τις ευπάθειες συγκεκριμένων προϊόντων IoT και έχουν την ικανότητα και δυνατότητα να αποκτήσουν παράνομα πρόσβαση, να αποθηκεύσουν ή να αναδιανείμουν πνευματική ιδιοκτησία και ευαίσθητα στοιχεία όπως έγγραφα, πηγαίο κώδικα, διαπιστευτήρια και άλλα απόρρητα αρχεία. [26]

IP theft	
Malicious actors may be able to illegally acquire, exploit, store or redistribute intellectual property and sensitive pieces of information (e.g. design documents, source code, credentials or other secrets). These provide dangerous insight into the vulnerabilities of the specific IoT products and may serve as valuable assets for attackers. This threat is closely related to the security-by-obscurity strategy (i.e. achieving security by ensuring documentation and sources remain secret) whose effectiveness and relevance is regularly criticized by experts.	• Product design. • Component manufacturing.

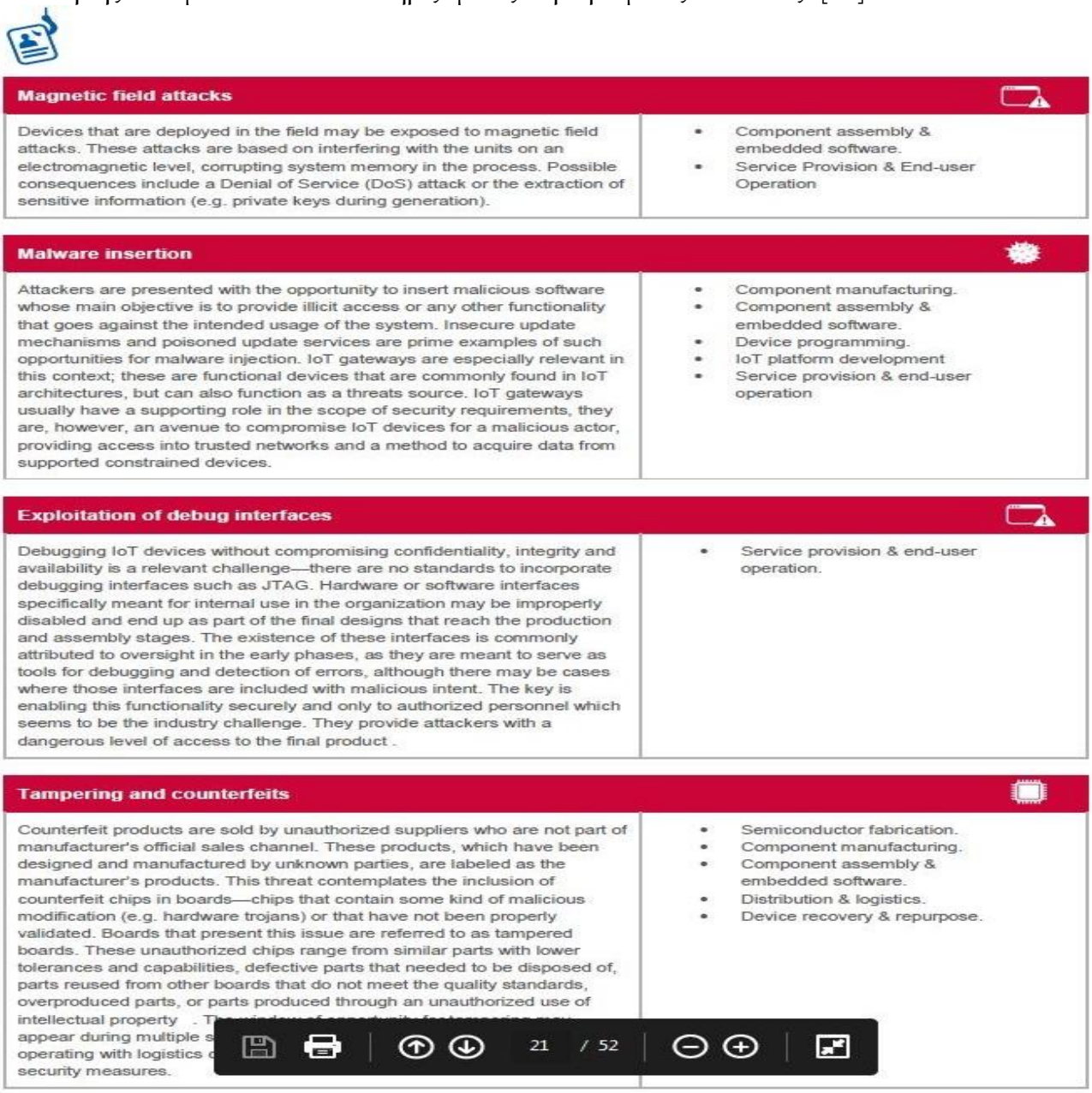
Reverse engineering	
The consequences of reverse engineering are arguably similar to those of IP theft; the main difference resides in the method used to obtain the sensitive assets and pieces of information (e.g. source code from the binaries, deep understanding of hardware blocks). These are derived from trial-and-error and meticulous study of the behaviour of a final product during the utilization phase by attackers that lack access to the original designs. This process may also lead to the discovery and release into the public domain of vulnerabilities (whether in first or third-party components) or firmware backdoors. It is important to note that reverse engineering in itself is not a threat, and should only be considered as such when used with malicious intent.	• Component assembly & embedded software. • Device programming. • Technical support & maintenance. • Device disposal & decommissioning.

Overproduction and cloning	
Overproducing is the practice of fabricating a product whose design documents and specifications have been provided willingly by the rightful owner, with the particularity that this is done outside of the established bounds of a legal contract. These products appear to be original but are insecure and pose a threat to the supply chain. A malicious factory can also clone the physical characteristics, firmware/software and security configuration of the device. Deployed devices might also be compromised and their software reverse-engineered, allowing for cloning. Cloned devices may be sold cheaply in the market and can contain functional modifications including backdoors. Alternatively, a genuine device may be substituted with a variant or clone during transportation or commissioning .	• Component manufacturing. • Component assembly & embedded software.

Εικόνα 12 Επιθέσεις πνευματικής ιδιοκτησίας [26]

7.3 Παράνομες ενέργειες και κατάχρηση

Οι συσκευές IoT ενδέχεται να εκτεθούν σε επιθέσεις μαγνητικού πεδίου. Αυτές οι επιθέσεις βασίζονται στην παρέμβαση στις μονάδες σε ηλεκτρομαγνητικό επίπεδο, περιλαμβάνουν επίθεση άρνησης υπηρεσίας DoS ή εξαγωγή ευαίσθητων πληροφοριών όπως ιδιωτικά κλειδιά κατά τη δημιουργία τους). Οι επιτιθέμενοι έχουν την ευκαιρία να εισάγουν κακόβουλο λογισμικό με κύριο στόχο την παράνομη πρόσβαση και λειτουργικότητας του συστήματος.
Οι πύλες IoT είναι ιδιαίτερα σχετικές σε αυτό το πλαίσιο. Αυτές είναι λειτουργικές συσκευές που βρίσκονται συνήθως σε αρχιτεκτονικές IoT, αλλά μπορούν επίσης να λειτουργήσουν ως πηγή απειλών. Οι πύλες IoT έχουν συνήθως υποστηρικτικό ρόλο στο πεδίο εφαρμογής των απαιτήσεων ασφαλείας, ωστόσο, αποτελούν έναν τρόπο συμβιβασμού συσκευών IoT για έναν κακόβουλο παράγοντα, παρέχοντας πρόσβαση σε αξιόπιστα δίκτυα και μια μέθοδο απόκτησης δεδομένων από υποστηριζόμενες περιορισμένες συσκευές. [26]



Magnetic field attacks	
Devices that are deployed in the field may be exposed to magnetic field attacks. These attacks are based on interfering with the units on an electromagnetic level, corrupting system memory in the process. Possible consequences include a Denial of Service (DoS) attack or the extraction of sensitive information (e.g. private keys during generation).	• Component assembly & embedded software. • Service Provision & End-user Operation

Malware insertion	
Attackers are presented with the opportunity to insert malicious software whose main objective is to provide illicit access or any other functionality that goes against the intended usage of the system. Insecure update mechanisms and poisoned update services are prime examples of such opportunities for malware injection. IoT gateways are especially relevant in this context; these are functional devices that are commonly found in IoT architectures, but can also function as a threats source. IoT gateways usually have a supporting role in the scope of security requirements, they are, however, an avenue to compromise IoT devices for a malicious actor, providing access into trusted networks and a method to acquire data from supported constrained devices.	• Component manufacturing. • Component assembly & embedded software. • Device programming. • IoT platform development • Service provision & end-user operation

Exploitation of debug interfaces	
Debugging IoT devices without compromising confidentiality, integrity and availability is a relevant challenge—there are no standards to incorporate debugging interfaces such as JTAG. Hardware or software interfaces specifically meant for internal use in the organization may be improperly disabled and end up as part of the final designs that reach the production and assembly stages. The existence of these interfaces is commonly attributed to oversight in the early phases, as they are meant to serve as tools for debugging and detection of errors, although there may be cases where those interfaces are included with malicious intent. The key is enabling this functionality securely and only to authorized personnel which seems to be the industry challenge. They provide attackers with a dangerous level of access to the final product .	• Service provision & end-user operation.

Tampering and counterfeits	
Counterfeit products are sold by unauthorized suppliers who are not part of manufacturer's official sales channel. These products, which have been designed and manufactured by unknown parties, are labeled as the manufacturer's products. This threat contemplates the inclusion of counterfeit chips in boards—chips that contain some kind of malicious modification (e.g. hardware trojans) or that have not been properly validated. Boards that present this issue are referred to as tampered boards. These unauthorized chips range from similar parts with lower tolerances and capabilities, defective parts that needed to be disposed of, parts reused from other boards that do not meet the quality standards, overproduced parts, or parts produced through an unauthorized use of intellectual property . T appear during multiple s operating with logistics security measures.	• Semiconductor fabrication. • Component manufacturing. • Component assembly & embedded software. • Distribution & logistics. • Device recovery & repurpose.

21 / 52

Εικόνα 13 Παράνομες ενέργειες [26]

7.4 Θέσπιση νομοθεσίας και προτύπων

Η αρχιτεκτονική των διαδικασιών γύρω από το απόρρητο και την κρυπτογράφηση είναι μια πρόκληση που επηρεάζεται από τους υπάρχοντες νόμους και κανονισμούς περί απορρήτου και από το γεγονός ότι ορισμένοι φορείς του οικοσυστήματος της αλυσίδας εφοδιασμού έχουν τη δική τους διαφορετική κατανόηση σχετικά με τις πτυχές ασφάλειας. Οι SLA υπογράφονται μεταξύ διαφορετικών παραγόντων στην αλυσίδα εφοδιασμού για να διασφαλιστεί μια κοινή συμβατική επιβολή των πτυχών ασφάλειας. Όλες οι συσκευές πρέπει να συμμορφώνονται με τις οδηγίες ασφαλείας που επιβάλλονται από αντίστοιχους κλάδους όπως της ενέργειας, της ιατρικής, της αυτοκινητοβιομηχανία. Επιπλέον, ο GDPR και οποιοιδήποτε άλλοι τοπικοί κανονισμοί πρέπει να εφαρμόζονται για την κάλυψη των κινδύνων που σχετίζονται με τη μη συμμόρφωση με πρότυπα και κανονισμούς. [26]

Implications due to standard and regulation non-compliance	
Architecting processes around privacy/encryption is a challenge that is affected by existing privacy laws and regulations and by the fact that some actors in the supply chain ecosystem have their own different understanding about the security aspects. SLAs are signed between different actors in the supply chain to ensure a common contractual enforced view of the security aspects. All devices should comply with security guidelines mandated by respective industries (e.g. energy, medical, automotive). Moreover, GDPR and any other local regulation should be applied to cover the risks associated with standards/regulation non-compliance.	• Product design. • Service provision & end-user operation. • Technical support & maintenance.

Εικόνα 14 Νομοθεσία και πρότυπα [26]

7.5 Απώλεια πληροφοριών

Τα συστήματα IoT που είναι απαραίτητα για τον έλεγχο των διαδικασιών εφοδιαστικής αλυσίδας και υπάρχουν σε ένα δίκτυο θα μπορούσαν να τεθούν σε κίνδυνο χωρίς τις κατάλληλες πολιτικές QoS ή τείχους προστασίας. Οι συσκευές που απαιτούν έλεγχο ταυτότητας δεν πρέπει ποτέ να έχουν τα εργοστασιακά διαπιστευτήρια ή διαπιστευτήρια που προέρχονται από εύκολα αποκτώμενες πληροφορίες. Τα συστήματα που σχετίζονται με οποιονδήποτε τρόπο με τη λειτουργία της αλυσίδας εφοδιασμού θα πρέπει ιδανικά να παρακολουθούνται εκτενώς για έγκαιρη ανίχνευση υλικού σε θέματα λογισμικού. Μια πιο προληπτική προσέγγιση για την ανίχνευση συνήθως οδηγεί σε μειωμένο αριθμό διαταραχών στην αλυσίδα εφοδιασμού, ειδικά σε σύγκριση με αντιδραστικά μέτρα.

Οι χρήστες πρέπει να ενημερώνονται και να εκπαιδεύονται κατάλληλα για να ευαισθητοποιηθούν σχετικά με τη λειτουργικότητα και τους κινδύνους ασφαλείας. είτε στην περίπτωση εσωτερικών μελών ενός οργανισμού που χρησιμοποιεί κρίσιμα συστήματα και εργαλεία αλυσίδας εφοδιασμού, είτε τελικούς χρήστες των οποίων οι συσκευές που έχουν

παραβιαστεί θα μπορούσαν να χρησιμοποιηθούν για να αποκτήσουν πρόσβαση σε άλλους κόμβους που θα μπορούσαν να διαταράξουν την αλυσίδα εφοδιασμού. [26]

Compromise of Network	
Systems that are necessary for the control of supply chain processes and exist in a network could become compromised without the proper QoS or firewall policies. These assets could be weaponized to orchestrate, for example, large scale Denial of Service (DoS) attacks, or to degrade the operation of the supply chain. Those that have access to the Internet are the most vulnerable, although isolated internal networks are also at risk from insider attacks.	• Product design. • Device programming. • Service provision & end-user operation.

Use of factory authentication settings	
Devices which require authentication should never leave the factory with a fixed global default credentials or a credentials derived from easily obtainable information (i.e. MAC address). Each device should have a unique random credentials assigned to it during manufacturing. Especially during any updates, which represent an important critical point in security.	• Product design. • Component assembly & embedded software. • Device programming. • Service provision & end-user operation • Technical support & maintenance.

Undetected software or hardware disruptions of the devices	
Systems related in any fashion to the operation of the supply chain should ideally be extensively monitored for an early detection of hardware of software issues. A more proactive approach on detection usually results in a reduced number of disruptions to the supply chain, especially when compared with reactive measures.	• All stages.

User Errors	
Users should be properly informed and trained to raise awareness about the functionality and the security risks; whether in the case of internal members of an organization operating critical supply chain systems and tools, or end users whose compromised devices could be used to gain access to other nodes that could disrupt the supply chain. Unintentional human errors could be the most direct approach to infiltrating into an otherwise adequately protected system. The interception of communications to other stakeholders related to the supply chain (e.g. procurements) and other attacks that derive from social engineering techniques are important threats to be considered in the context of user errors.	• Service provision & end-user operation. • Technical support & maintenance. • Device recovery & repurpose.

Attack to registration procedures	
A lack of registration procedures, or insecure registration mechanisms, could lead to attackers registering fraudulent devices or preventing the registration of genuine devices. Devices must be registered in the appropriate authentication IoT platform services after device initialization in the product line and before final user provisioning in order to grant them access.	• Device programming. • IoT platform development. • Service provision & end-user operation. • Technical support & maintenance.

Use of recovered or repurposed components	
Organizations may opt to reuse components or parts that have already gone through the regular supply chain flow; this could be done for reasons such as cost optimization. The usage of components that have already been retired and may have not been properly validated for reinsertion in the supply chain poses a threat and could contaminate an otherwise secure batch of devices.	• Device recovery & repurpose.

Attack to manufacturing processes	
Manufacturing pipelines are highly sensitive points of entry to the supply chain. Processes that do not implement adequate measures to regulate and monitor the access of personnel to the pipeline could cause serious vulnerabilities; this could in turn lead to other discussed threats such as sabotage or malware injection.	• Semiconductor fabrication. • Component manufacturing. • Component assembly & embedded software.

Εικόνα 15 Απώλεια πληροφοριών [26]

8 Καλές πρακτικές ασφάλειας της αλυσίδας IoT

Σε αυτή την ενότητα θα αναλυθούν όλες οι εκτιμήσεις ασφάλειας σχετικά με την IoT αλυσίδα και οι καλές πρακτικές για την βελτίωση της ασφάλειας.

8.1 Εκτιμήσεις ασφάλειας στην IoT αλυσίδα

Ένας από τους σημαντικότερους στόχους είναι η αντιμετώπιση των κύριων ζητημάτων ασφάλειας που πρέπει να υιοθετηθούν σε όλη την αλυσίδα εφοδιασμού για το IoT. Στον παρακάτω πίνακα παρουσιάζεται ένας κατάλογος με θέματα ασφαλείας. Ένα ζήτημα ασφάλειας που εφαρμόζεται με οριζόντιο τρόπο σε όλα τα στάδια είναι το γεγονός ότι αυτές οι διαδικασίες που είναι πέρα από τον άμεσο έλεγχο του οργανισμού είναι εγγενώς προκλητικές · Οι έλεγχοι και οι επιθεωρήσεις μπορούν να βοηθήσουν σε αυτό το ζήτημα, αλλά είναι δύσκολο να εφαρμοστούν. Ένα άλλο οριζόντιο ζήτημα ασφάλειας μπορεί να βρεθεί στην ανθεκτικότητα της αξιοπιστίας της αλυσίδας εφοδιασμού, δηλαδή της ικανότητας παροχής συνεχούς υπηρεσίας λειτουργίας. [26]

Stages	Security considerations	Description
Product design	Threat model	Identification and creation of a catalogue of potential threats.
	Secure building blocks	Usage of up-to-date and properly supported building blocks (e.g. cryptography, software libraries).
	Sabotage prevention	Monitoring of deliberate flaws in design introduced by insider threats.
	Physical-logical convergence	Ensuring adequate visibility of all requirements and needs for security engineers and other stakeholders (especially relevant in E2E security design).
	Recovery plan	Conceptual design must face and consider the definition of a recovery plan for future stages and secure mechanisms to implement it (compliant with the chain of trust).
	Combined security controls (SW and tamper resistant HW)	Define the integration between HW and SW when defining security measures. Security controls (e.g. secure boot, attestation) require the usage of tamper resistant hardware to fulfil the security requirements.
	Chain of trust definition	Chain of trust is necessary to ensure levels of trust between HW and SW elements.
	Resource constraints	Achieving a compromise between device resources (e.g. memory, computation) and other constraints such as cost or size that ensures devices are able to implement security measures while leaving room for future unexpected developments.

Semiconductor Fabrication	Hardware security mechanism	Integration of a hardware root of trust to serve as the trusted secure foundation of cryptographic operations.
	Scrap management	Management of residual and discarded materials to ensure parts are securely removed from the supply chain.
Component Manufacturing	Counterfeit components	Usage of authenticated parts to avoid security concerns introduced by fraudulent components.
	Defective components	Usage of properly tested parts that pass the quality requirements to avoid degradation of security.
Component Assembly + Embedded Software	Firmware access control	Enable secure mechanisms to control access to firmware for updates and other maintenance operations. Specially for its installation.
	Backdoors	Monitoring of suspicious behaviour and backdoors implanted in hardware or low-level firmware boot code.
Device Programming	Secure provisioning	Usage of end-to-end robust provisioning mechanisms guaranteeing the security of credentials and cryptographic information.
	Coding practices	Adoption of best practices such as code reviews and continuous integration of cybersecurity checks in the software development process.
IoT Platform Development	Development focus	Basing development efforts on a risk-based approach to achieve both adequate functionality and security.
	Dependencies management	Checks and review processes to ensure that dependencies and libraries are available, have not been tampered with and conform to security requirements.
	Network security	Secure network policies to minimize the risk of intrusion while exposing the required services in the public domain.
Service Provision & End-user Operation	Management support	Appropriate level of resources and support provided by the organization to ensure secure operation during the lifecycle of the IoT device.
	Convenience compromises	Appropriate balance of user convenience and intrusive security mechanisms that degrade the user experience.
	Usage by operators	Operators of IoT services are provided with adequate training to avoid introducing security risks that originate from misuse or misconfiguration.
	Adoption of security features	Monitoring and usage of techniques to increase the adoption rate of optional security features by end users.
	Technical support	Technical support throughout the life cycle of the product.
	Access control	Management of credentials (including revocation) and access permissions of devices to IoT platforms.

Distribution and logistics	Value-added resellers (VAR)	Certification of personalization services for IoT devices offered by third parties that may introduce unforeseen security risks.
	Protection against theft and counterfeits	Adoption of security measures to reduce the risk of property theft and replacement with counterfeit components in the distribution process and logistics chain.
	Device identity	Compose a device identity during device fabrication based on the combination of the different HW and SW components (e.g. board ID, secure element ID). This device identity composition helps to track and device fabrication tracking and can be used in the IoT platform access control.
	Tracking for registration	Define a proper device registration or onboarding to the IoT platform based on the tracking of the device in the different stages of fabrication.
Technical Support & Maintenance	OTA control tools	Adoption of mechanisms to ensure remote Over-The-Air control tools used for maintenance are properly managed and secured following the chain of trust.
	Patches	Usage of software version that sufficiently mitigates the threats exposed and the latest security patches to avoid risks from well-known security vulnerabilities.
Device Recovery & Repurpose	Data removal	Adoption of secure data removal techniques to avoid sensitive pieces of information remaining on the device.

Εικόνα 16 Στάδια εκτίμησης ασφάλειας [26]

8.2 Καλές πρακτικές βελτίωσης ασφάλειας στην IoT αλυσίδα

Η ανάπτυξη ορθών πρακτικών για την εξασφάλιση και βελτίωση της ασφάλειας της αλυσίδας εφοδιασμού IoT είναι ένας από τους βασικούς στόχους αυτής της μελέτης. Ο στόχος είναι να παρέχονται οδηγίες για την καλύτερη δυνατή αντιμετώπιση και τον μετριασμό των απειλών που ενδέχεται να επηρεάσουν την αλυσίδα εφοδιασμού IoT. Για να οργανώσετε τους τομείς με λογικό τρόπο, οι καλές πρακτικές ταξινομήθηκαν στις ακόλουθες τρεις κύριες ομάδες:

- Λήψη πρακτικών για την διασφάλιση ασφάλειας
- Διαδικασίες για την διασφάλιση της ασφάλειας
- Τεχνολογίες για την διασφάλιση της ασφάλειας

8.3 Λήψη πρακτικών για την διασφάλιση ασφάλειας

8.3.1 Η συνεργασία σας να είναι με προμηθευτές που παρέχουν εγγυήσεις ασφάλειας

Η συνεργασία με εξωτερικούς προμηθευτές λόγω της έλλειψης ελέγχου στα μέτρα ασφαλείας τους περιλαμβάνει ένα σημαντικό κίνδυνο για την ασφάλεια. Αυτό ο κίνδυνος μπορεί να ελαχιστοποιηθεί όταν συνεργαζόμαστε με εταιρείες που εφαρμόζουν πρότυπα όπως τα ISO 27036 και ISO 28000, ή συστάσεις όπως το NISTIR 8259.10. Μια εταιρεία που ζητά έγκριση πιστοποίησης είναι συνήθως ένα σημάδι ότι είναι πρόθυμες να εργαστούν σοβαρά για τη βελτίωση της ασφάλειας της εφοδιαστικής αλυσίδας. Η πιστοποίηση είναι συνήθως μια δαπανηρή διαδικασία που δεν είναι κατάλληλη για όλους τους οργανισμούς που δεν είναι τυποποιημένοι αλλά έχουν ολοκληρωμένα μέτρα ασφαλείας και είναι διαφανείς σχετικά με αυτά [26]

8.3.2 Προσπάθεια για συνεχή βελτίωση της διαφάνειας

Η διαφάνεια είναι ζωτικής σημασίας για τον έλεγχο της ασφάλειας στην εφοδιαστική αλυσίδα. Τα ενδιαφερόμενα μέρη, ιδίως οι προμηθευτές, πρέπει να είναι διαφανή, προσφέροντας σαφείς και λεπτομερείς πληροφορίες σχετικά με τις λειτουργίες και την κανονική συμπεριφορά των παρεχόμενων προϊόντων. και επικοινωνία όλων των σχετικών πληροφοριών στο επόμενο βήμα της αλυσίδας. Ένα αυξημένο επίπεδο διαφάνειας θα έχει την επιθυμητή παρενέργεια της ενίσχυσης της εμπιστοσύνης μεταξύ των συμμετεχόντων στην αλυσίδα εφοδιασμού. [26]

8.3.3 Ανάπτυξη σε κοινότυπα πρότυπα εμπιστοσύνης

Η εμπιστοσύνη μεταξύ των ενδιαφερομένων είναι μια από τις πιο σχετικές και σημαντικές προκλήσεις που πρέπει να ληφθούν υπόψη για την ασφάλεια της αλυσίδας εφοδιασμού IoT Κάθε ενδιαφερόμενος πρέπει να καθιερώσει ένα ελάχιστο επίπεδο εμπιστοσύνης σύμφωνα με τις ανάγκες και την εμπειρογνωμοσύνη, αναλύοντας τη ροή δεδομένων και εγγυώντας την ασφάλεια και το απόρρητο στις υπηρεσίες των προϊόντων τους. Τα μοντέλα εμπιστοσύνης ορίζουν ένα πλαίσιο για την παροχή επίσημων εγγυήσεων σχετικά με τη συμπεριφορά των διαφόρων μερών και την ενίσχυση της ασφάλειας. Η αλυσίδα εφοδιασμού θα επωφεληθεί σημαντικά από την ανάπτυξη καινοτόμων μοντέλων εμπιστοσύνης ή την προσαρμογή των υφιστάμενων, θα πρέπει να σημειωθεί ότι δεν υπάρχει μια κατάλληλη προσέγγιση για την εμπιστοσύνη. Μια προσέγγιση που βασίζεται σε συνεπή αξιολόγηση κινδύνου θα επέτρεπε στους οργανισμούς να αξιολογήσουν τον επιχειρηματικό αντίκτυπο για να εφαρμόσουν τα κατάλληλα τεχνικά μέτρα και τις συμβατικές υποχρεώσεις. [26]

8.3.4 Υιοθέτηση της ασφάλειας στην αλυσίδα εφοδιασμού ως μόνιμη διαδικασία

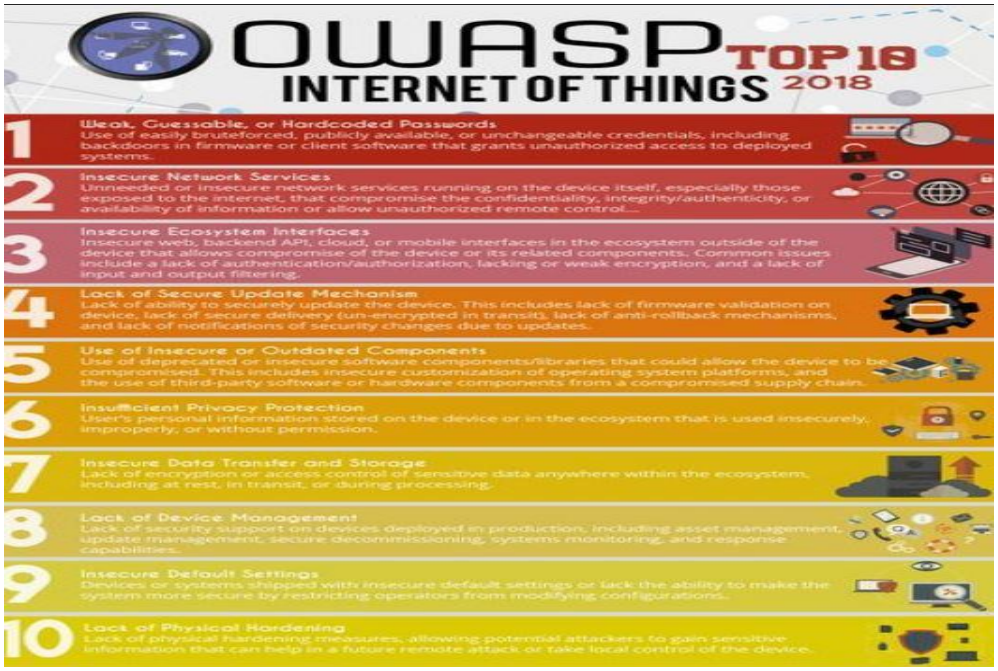
Η ασφάλεια στην αλυσίδα εφοδιασμού δεν πρέπει να χαρακτηρίζεται ως περιστασιακή δραστηριότητα. Οι διαβεβαιώσεις που παρέχονται από ενέργειες στο επίπεδο ασφάλειας όπως δοκιμές διείσδυσης (Penetration Test) μειώνουν την αξία με την πάροδο του χρόνου μετά τη λήψη τους. Η έννοια μιας διαδικασίας συνεπάγεται ροή και επίσημη συναίνεση μεταξύ των ενδιαφερομένων, καθώς και έγκριση και αποδοχή. Η ασφάλεια πρέπει να συμπεριληφθεί σε όλα τα στάδια της εφοδιαστικής αλυσίδας ως συνεχής και επαναληπτική διαδικασία. [26]

8.3.5 Εκπαίδευση και διαχείριση ενός εξειδικευμένου εργατικού δυναμικού

Όπως συμβαίνει με πολλά τεχνολογικά πεδία, ο τομέας IoT εμφανίζει γρήγορο ρυθμό αλλαγής. Η διατήρηση ενός εξειδικευμένου εργατικού δυναμικού που έχει πρόσβαση σε τακτική εκπαίδευση ασφάλειας και οι απαιτούμενοι πόροι για να ενημερώνεται σχετικά με τον τομέα έχει μεγάλη σημασία για την αντιμετώπιση των προκλήσεων ασφάλειας που θέτει η αλυσίδα εφοδιασμού για το IoT. Επαγγελματικές ομάδες αφιερωμένες αποκλειστικά στην ασφάλεια πρέπει να είναι παρόντες στους περισσότερους οργανισμούς Εκείνοι που δεν διαθέτουν τους πόρους για να διατηρήσουν τέτοιες ομάδες θα πρέπει τουλάχιστον να διασφαλίσουν ότι άλλες τεχνικές ομάδες έχουν τον κατάλληλο βαθμό γνώσεων σχετικά με την ασφάλεια. [26]

8.3.6 Προώθηση μιας κουλτούρας στην εργασία μας που εστιάζει στον κίνδυνο

Οι προγραμματιστές λογισμικού τείνουν μερικές φορές να επενδύουν σημαντικούς πόρους στην επιδίωξη εκτεταμένης λειτουργικότητας για το τελικό προϊόν, το οποίο μπορεί να έχει την ανεπιθύμητη παρενέργεια της λήψης των εν λόγω πόρων από εργασίες που σχετίζονται με την ασφάλεια. Αυτό το ζήτημα μπορεί να επιδεινωθεί από ορισμένες αποφάσεις από τα επίπεδα διαχείρισης, εάν αποσυνδεθούν από την εστίαση ανάπτυξης. Η προώθηση μιας διαδικασίας ανάπτυξης που λαμβάνει υπόψη τους κινδύνους κατά τη διανομή πόρων και διασφαλίζει ότι η ασφάλεια λαμβάνει την κατάλληλη προσοχή μπορεί να έχει σημαντικό αντίκτυπο στην ασφάλεια της αλυσίδας εφοδιασμού. Στην παρακάτω εικόνα παρουσιάζονται τα δέκα κορυφαία θέματα για την ασφάλεια των IoT συσκευών σύμφωνα με τον μη κερδοσκοπικό οργανισμό ασφάλειας OWASP. Αυτά είναι τα πιο κοινά τρωτά σημεία του συστήματός μας και μπορούμε εύκολα να αυξήσουμε το επίπεδο ασφάλειας είτε σε επίπεδο χρήστη είτε σε επίπεδο ομάδα ασφαλείας με συγκεκριμένες ενέργειες αντιστοίχως. [26]



Εικόνα 17 10 κορυφαία θέματα ασφάλειας που παρουσιάζονται από τον OWASP

8.3.7 Ενημερωτικά προγράμματα στους χρήστες για την ασφάλεια

Οι χρήστες δεν έχουν γνώση σχετικά με την ασφάλεια και τις συνέπειες της αδύναμης ασφάλειας. Οι ευάλωτες συσκευές IoT των χρηστών μπορούν να χρησιμοποιηθούν για να αποκτήσουν πρόσβαση σε συστήματα και υπηρεσίες στην αλυσίδα εφοδιασμού. Οι οργανισμοί θα πρέπει να δώσουν πόρους για εκστρατείες και προγράμματα για να την ενημέρωση για την ασφάλεια. Οι χρήστες θα εκπαιδεύονται ώστε να λαμβάνουν όλα τα μέτρα που μπορούν για την βέλτιστη ασφάλεια χωρίς να αφεθεί απλά η ευθύνη σε αυτούς. Στους πελάτες πρέπει να παρέχονται σαφείς και ρητές πληροφορίες σχετικά με την ασφάλεια. Αυτό περιλαμβάνει, για παράδειγμα, πιθανές ευπάθειες που θα μπορούσαν να εντοπιστούν κατά τη διάρκεια του κύκλου ζωής του προϊόντος ή τη σχέση ενημερώσεων λογισμικού που αναπτύσσονται σε συσκευές στο πεδίο. Η μεταφορά αυτών των πληροφοριών σε παράγοντες της αλυσίδας είναι ζωτικής σημασίας για την επίτευξη συνεχούς ασφάλειας. [26]

8.4 Διαδικασίες για την διασφάλιση της ασφάλειας

8.4.1 Έγκριση ασφάλειας από αρχές σχεδιασμού

Η ασφάλεια πρέπει να βρίσκεται σε υψηλή προτεραιότητα και να υπολογίζεται κατά τον σχεδιασμό από τα πρώτα στάδια και σε ολόκληρη την αλυσίδα εφοδιασμού. Η ενσωμάτωση μιας ισχυρής αλυσίδας εμπιστοσύνης θα πρέπει να αποτελεί προτεραιότητα για τη διασφάλιση της ακεραιότητας των μονάδων υλικού και λογισμικού σε συσκευές IoT. Ένα μοντέλο ασφάλειας πρέπει να καλύπτει τα βασικά στοιχεία όπως η προστασία, η ανίχνευση και η

απόκριση συμβάντων. Μια άλλη σημαντική πρακτική είναι η συμπερίληψη νομικών τμημάτων στις αξιολογήσεις ασφάλειας και απορρήτου. Επιπλέον, οι εμπειρογνώμονες ασφαλείας θα πρέπει να συμμετέχουν άμεσα στις πρώιμες συζητήσεις σχεδιασμού με την ομάδα διαχείρισης προϊόντων, ώστε να μπορούν να συμπεριλάβουν την άποψή τους στην επιλογή των υλικών σύμφωνα με τις απαιτήσεις ασφαλείας τους. [26]

8.4.2 Εγκατάσταση και βελτίωση συλλογής δεδομένων, τεχνολογίες μέτρησης και διαχείριση δεδομένων

Επειδή δεν είναι εφικτό να υπάρχουν οι πόροι για τη διενέργεια ελέγχων ασφαλείας ή ανάλυσης, επομένως η πλειοψηφία εκτελεί παραδοχές εμπιστοσύνης. .Είναι επιθυμητό να ελαχιστοποιηθούν αυτές οι υποθέσεις όταν είναι εφικτό, διατηρώντας παράλληλα τις εγγυήσεις απορρήτου για τον τελικό χρήστη. Ένα προηγμένο εργαλείο ή μηχανισμός για τη συλλογή και τη μέτρηση των δεδομένων θα ήταν σημαντική βοήθεια σε αυτό το θέμα. Πρωτοβουλίες όπως οι Διεθνείς Χώροι Δεδομένων μια διεθνής πρωτοβουλία με συνδέσμους προς την Ευρωπαϊκή Επιτροπή που επικεντρώνεται στη βελτίωση μεθόδων και μηχανισμών για μια πιο ασφαλή και αξιόπιστη ανταλλαγή δεδομένων στα επιχειρηματικά οικοσυστήματα - μπορεί επίσης να δώσει έμπνευση. [26]

8.4.3 Δημιουργία μέτρων ασφάλειας αλυσίδας παροχής

Η έννοια της ακεραιότητας στο πλαίσιο της αλυσίδας εφοδιασμού IoT είναι αναμφισβήτητα πολύ ευρεία. Οι περισσότερες ερμηνείες θα μπορούσαν να συμφωνήσουν ότι σχετίζεται με την κατάσταση της αλυσίδας εφοδιασμού που λειτουργεί με μη τροποποιημένο τρόπο, ότι είναι απαλλαγμένη από πλαστά, κακόβουλα προγράμματα ή άλλες επιρροές που ενδέχεται να μειώσουν την ορατότητα και την υπευθυνότητα. Οι μετρήσεις μπορούν να δημιουργηθούν και να παρακολουθούνται συνεχώς για να παρέχουν ορατότητα στην κατάσταση της αλυσίδας εφοδιασμού. Αυτές οι μετρήσεις θα μπορούσαν να συνδεθούν με τις ιδιαιτερότητες της τρέχουσας αλυσίδας εφοδιασμού ή να έχουν περισσότερο οριζόντιο χαρακτήρα. Οι μετρήσεις θα μπορούσαν να σχεδιαστούν κυρίως στις προηγούμενες φάσεις σχεδιασμού και να προσαρμοστούν με επαναληπτικό και συνεχή τρόπο ανάλογα με την εξέλιξη της αλυσίδας εφοδιασμού. Παραδείγματα τέτοιων μετρήσεων θα μπορούσαν να περιλαμβάνουν τη διανομή εκδόσεων υλικολογισμικού που χρησιμοποιούνται αυτήν τη στιγμή στο πεδίο. [26]

8.4.4 Ανάπτυξη μοντέλων απειλής για την αλυσίδα παροχής IoT

Τα μοντέλα απειλής θα πρέπει να συγχωνεύσουν τις έννοιες τόσο της φυσικής ασφάλειας όσο και της ψηφιακής ασφάλειας που είναι εγγενείς στα κυβερνο-φυσικά συστήματα. Η διαδικασία ανάπτυξης περιλαμβάνει τον διαχωρισμό της αλυσίδας εφοδιασμού σε λειτουργικά μπλοκ και

την καταχώριση των περιουσιακών στοιχείων σε αυτά τα μπλοκ, για την ανίχνευση κρίσιμων περιουσιακών στοιχείων και μπλοκ. Για το σκοπό αυτό, μια γνωστική βάση τακτικών και τεχνικών επίθεσης όπως το MITER ATT & CK ή το μοντέλο απειλής που παρουσιάζεται σε αυτήν την έκθεση μπορεί να χρησιμεύσει ως το θεμέλιο για την ανάπτυξη συνδυασμένων μοντέλων απειλής (ασφάλειας-ασφάλειας). Αυτό πρέπει επίσης να περιλαμβάνει, εκτός από απειλές επιθέσεων, ακούσια περιστατικά που μπορεί επίσης να επηρεάσουν την ασφάλεια και την απόδοση που προκύπτουν από σφάλματα στη διαχείριση της αυξημένης πολυπλοκότητας των συστημάτων που προέρχονται από την προσθήκη του IoT. Η μεθοδολογία εκτίμησης κινδύνων πρέπει να εφαρμοστεί προκειμένου να εκτιμηθεί η σχετική σημασία των απειλών ανάλογα με την κρίσιμη σημασία του τομέα και να εφαρμοστούν δράσεις (π.χ. βελτιστοποίηση των διαθέσιμων πόρων, προετοιμασία σχεδίων έκτακτης ανάγκης) για την προστασία των διαφόρων σταδίων της αλυσίδας εφοδιασμού - κίνητρο πίσω από το Οι επιθέσεις στον κυβερνοχώρο (π.χ. οικονομικό κέρδος, τρομοκρατία) θα πρέπει επίσης να εξεταστούν για να ορίσουν οικονομικά αποδοτική προστασία και ελέγχους ασφαλείας. Επιπλέον, ένας σημαντικός αριθμός στοιχείων IoT παρουσιάζει έλλειψη ευθύνης για τις εργασίες που εκτελούν. Αυτό οφείλεται στην απουσία σύνδεσης στις περισσότερες συσκευές IoT λόγω περιορισμών υλικού ή πρόσθετου κόστους. Θα πρέπει να πραγματοποιηθεί εκτίμηση κινδύνου για ολόκληρη τη ρύθμιση της αλυσίδας εφοδιασμού IoT για τον εντοπισμό εξαρτημάτων όπου απαιτούνται. [26]

8.4.5 Ταυτοποίηση λογισμικού τρίτων

Η χρήση λογισμικού τρίτου μέρους εισάγει ένα βαθμό αβεβαιότητας που δρα ως απειλή για την ασφάλεια της αλυσίδας εφοδιασμού. Αυτά τα στοιχεία λογισμικού πρέπει να τεκμηριώνονται ως μέρος της διαδικασίας ασφάλειας της εφοδιαστικής αλυσίδας, συμπεριλαμβανομένων των κριτηρίων που ακολουθούνται για την επιλογή του. οι οργανισμοί θα πρέπει να προτιμούν εκείνους που έχουν περάσει μια διαδικασία αξιολόγησης και πιστοποίησης και να περιλαμβάνουν σχέδιο συντήρησης. Συνιστάται μια ολοκληρωμένη ανάλυση του πηγαίου κώδικα για περιπτώσεις ανοιχτού κώδικα όπου δεν μπορεί να αναγνωριστεί μια αξιόπιστη κοινότητα συντηρητών και ενδιαφερόμενων φορέων - μια πιθανή προσέγγιση για την κάλυψη ευάλωτου κώδικα είναι η ανάπτυξη ενός προσαρμοσμένου επιπέδου στην κορυφή, αν και αυτό αναγκάζει τον οργανισμό να ακολουθήσει ενημερώσεις του αρχικού προγραμματιστή. Για να βοηθήσουν στη διαδικασία αναγνώρισης λογισμικού, οι οργανισμοί μπορούν να χρησιμοποιούν εργαλεία λογισμικού που ειδικεύονται στο Ανάλυση στοιχείων όπως το OWASP Dependency-Track, το οποίο είναι ένα εργαλείο για τη δημιουργία SBOMs (ανατρέξτε στη σχετική πρακτική PRO-13). Τα προϊόντα σάρωσης μπορεί επίσης να αξιοποιηθούν για τον εντοπισμό στοιχείων και τρωτών σημείων λογισμικού. Τα εργαλεία σάρωσης πηγαίου κώδικα είναι διαθέσιμα για στοιχεία εσωτερικού και ανοιχτού κώδικα, ενώ εργαλεία δυαδικής σάρωσης μπορούν να εφαρμοστούν στο πλαίσιο κλειστής πηγής. Πρέπει να σημειωθεί ότι τα εργαλεία ανοιχτού κώδικα μπορούν να διαδραματίσουν σημαντικό ρόλο στην ασφάλεια του IoT, καθώς η διαφάνεια και η διαφάνεια είναι πολύ σημαντικές. Η κοινότητα ανοιχτού κώδικα είναι επίσης αποτελεσματική κατά την εύρεση ελαττωμάτων και την άμεση διόρθωσή τους. Ο

κλάδος ωφελείται σημαντικά όταν οι διορθώσεις για ευπάθειες που εντοπίζονται σε εργαλεία ανοιχτού κώδικα στο πλαίσιο ενός ιδιωτικού οργανισμού επιστρέφονται στην κοινότητα ανοιχτού κώδικα. [26]

8.4.6 Εγκατάσταση συνολικού σχεδίου δοκιμών

Όλες οι λύσεις IoT πρέπει να περιλαμβάνουν ένα ολοκληρωμένο σχέδιο δοκιμών για να επαληθεύσετε ότι το προϊόν εμφανίζει τις αναμενόμενες δυνατότητες τόσο στο λογισμικό όσο και στο υλικό. Ο έλεγχος αποδοχής πρέπει να πραγματοποιείται ανεξάρτητα από τυχόν προηγούμενες δοκιμές που θα μπορούσαν να είχαν πραγματοποιηθεί σε προηγούμενα στάδια της αλυσίδας εφοδιασμού. Ένα κλάσμα των συσκευών θα πρέπει να επιθεωρείται στο τελευταίο μέρος της κατασκευής και να υποβάλλεται σε έλεγχο ασφάλειας στον κυβερνοχώρο για τον εντοπισμό λανθασμένων διαμορφώσεων ή σφαλμάτων. [26]

8.4.7 Εφαρμογής που χρησιμοποιούνται ασφάλεια από την οριστική

Ένα σημαντικό ποσοστό των πελατών τείνουν να αγνοούν τα χαρακτηριστικά ασφαλείας για λόγους ευκολίας ή έλλειψης τεχνικών γνώσεων. Αυτό συνήθως οδηγεί σε ευπάθειες που θα μπορούσαν να αποφευχθούν με την κατάλληλη χρήση των δυνατοτήτων ασφαλείας που ήδη περιλαμβάνονται στις συσκευές και τα προϊόντα. Η ασφάλεια από προεπιλογή θα πρέπει να είναι η προσέγγιση για τους κατασκευαστές και τους προμηθευτές, έτσι οι πελάτες που πρέπει να απενεργοποιήσουν την ασφάλεια πρέπει να το πράξουν με συνειδητό και σαφή τρόπο. Αυτή η προσέγγιση θα βασίζεται σε ένα συνεπές μοντέλο ασφάλειας που είναι υποχρεωτικό να εφαρμόζεται και να διασφαλίζει ότι τα δεδομένα συλλέγονται, χειρίζονται και μεταφέρονται σωστά. [26]

8.4.8 Δέσμευση παροχής δελτίων ασφάλειας για ορισμένη περίοδο χρόνου

Οι παλαιές συσκευές IoT που βασίζονται σε μη χρωματισμένο λογισμικό αποτελούν απειλή για την ακεραιότητα της αλυσίδας εφοδιασμού. Η εκτεταμένη υποστήριξη και η έγκαιρη παράδοση ενημερωμένων εκδόσεων ασφαλείας πρέπει να ληφθούν υπόψη στο σχεδιασμό και τον σχεδιασμό ενός προϊόντος IoT - αυτό περιλαμβάνει την κατάλληλη διάσταση πόρων (π.χ. μνήμη) για την υποστήριξη μελλοντικών ενημερώσεων. Οι κατασκευαστές θα πρέπει να έχουν την υποχρέωση να παραδίδουν ενημερώσεις ασφαλείας τουλάχιστον μέχρι το τέλος της εγγύησης και κατά προτίμηση μέχρι το τέλος της περιόδου υποστήριξης. Σε κάθε περίπτωση, η χρονική περίοδος που ο κατασκευαστής δεσμεύεται να παρέχει τις ενημερώσεις ασφαλείας θα πρέπει να αναφέρεται ρητά και ξεκάθαρα πριν από την προμήθεια και να διατίθεται χωρίς επιπλέον κόστος κατά τη χρήση. [26]

8.4.9 Διαδικασίες διαχείρισης ασφαλής ασφάλειας

Τα υλικά και τα εξαρτήματα που παράγονται στα στάδια κατασκευής και κατασκευής που αποτυγχάνουν στις δοκιμές ποιότητας ή δεν θεωρούνται έτοιμα για παραγωγή για οποιονδήποτε πιθανό λόγο θα πρέπει να υποβάλλονται σε επεξεργασία και να απορρίπτονται με ασφαλή τρόπο (π.χ. αποφύγετε να αφήσετε τις ελαττωματικές μονάδες σε μη ασφαλή δοχεία). Αυτό γίνεται για να αποφευχθεί η απειλή κακόβουλων ηθοποιών να αποκτήσουν πρόσβαση σε αυτά τα εξαρτήματα, τα οποία θα μπορούσαν να κυκλοφορήσουν στην αγορά δωρεάν ή να χρησιμεύσουν ως πολύτιμα περιουσιακά στοιχεία για να μελετήσουν και να ανακαλύψουν ευπάθειες ή να παράγουν πλαστά μέσω της αντίστροφης μηχανικής. [26]

8.4.10 Χρήση ασφάλειας τεχνικών αφαίρεσης δεδομένων

Οι συσκευές συνήθως αποκαθίστανται στις εργοστασιακές ρυθμίσεις και διαγράφονται από όλα τα προσωπικά δεδομένα χρήστη κατά τη διάρκεια του σταδίου παροπλισμού και ανάκτησης. Οι μη ασφαλείς πρακτικές αφαίρεσης δεδομένων (π.χ. μια απλή διαδικασία διαγραφής που δεν αντικαθιστά όλους τους τομείς αποθήκευσης) ενδέχεται να αφήσουν ίχνη δεδομένων ιδιωτικού χρήστη στον μόνιμο χώρο αποθήκευσης που μπορεί αργότερα να ανακτηθούν χρησιμοποιώντας εξειδικευμένα εργαλεία λογισμικού από άλλο χρήστη με πρόσβαση στη συσκευή. Οι ασφαλείς τεχνικές διαγραφής δεδομένων πρέπει να ενσωματωθούν σε αυτά τα στάδια για να διασφαλιστεί ότι όλα τα προσωπικά δεδομένα χρήστη και τα δεδομένα διαμόρφωσης αφαιρούνται αποτελεσματικά με ασφαλή τρόπο. Ορισμένες από αυτές τις τεχνικές πρέπει να ληφθούν υπόψη πριν από την αφαίρεση δεδομένων, όπως η διαγραφή κρυπτογράφησης, που σημαίνει ότι αυτή η καλή πρακτική πρέπει να υιοθετηθεί από την αρχή της αλυσίδας εφοδιασμού. [26]

8.4.11 Δημιουργία συνολικών πόρων εγγραφής

Δημιουργήστε ένα ολοκληρωμένο σύνολο πόρων τεκμηρίωσης για την καταπολέμηση των ανθρώπινων σφαλμάτων που περιλαμβάνουν σαφείς οδηγίες ή σημεία δράσης για εφαρμογή σε κάθε παραδοτέο, ιδίως σχετικά με τις πτυχές της διαχείρισης διαμόρφωσης και της αποκατάστασης μετά από μια αποτυχία. Αυτό είναι ένα κρίσιμο ζήτημα καθώς η απουσία των εν λόγω πόρων αποτελεί απειλή για την αλυσίδα εφοδιασμού. Επιπλέον, η παρουσία τεκμηρίωσης υπό-ισοτιμίας θα μπορούσε πραγματικά να είναι ενεργά επιβλαβής. Τα στάδια υποστήριξης και στο τέλος του κύκλου ζωής τους είναι ιδιαίτερα ευάλωτα σε αυτήν την απειλή. Ο ENISA θα μπορούσε να διαδραματίσει σημαντικό ρόλο σε αυτό το θέμα φιλοξενώντας και διατηρώντας ένα αποθετήριο πόρων, όπως λίστα με λανθασμένες στοίβες λογισμικού που πρέπει να αποφεύγονται από τους πωλητές ή μια λίστα ασφαλών εξαρτημάτων και αποδεδειγμένων συνδυασμών που θα χρησιμοποιηθούν ως κατευθυντήρια γραμμή στο στάδιο του σχεδιασμού. [26]

8.4.12 Ανάπτυξη Ή προσαρμόστε πρότυπα για την αλυσίδα εφοδιασμού για IOT

Προς το παρόν κανένα πρότυπο δεν ταιριάζει απόλυτα στο σκοπό της διασφάλισης της αλυσίδας εφοδιασμού για IoT σε όλους τους κλάδους. Αν και θα μπορούσαν να εφαρμοστούν ορισμένα πρότυπα ασφάλειας πληροφορικής, υπάρχουν περιορισμοί, ανάλογα με τον κλάδο. Ορισμένα πρότυπα, όπως το ISO27001 ή το πρόσφατο NERC CIP-013-1, θα μπορούσαν αναμφισβήτητα να θεωρηθούν αρκετά ανοιχτά ή γενικά. Για ορισμένους τομείς ή κλάδους, ορισμένα πρότυπα είναι πολύ αφηρημένα και θεωρούνται δύσκολο να κατανοηθούν και να εφαρμοστούν στο πλαίσιο. Επιπλέον, υπάρχει αναμφισβήτητα ένα κενό μεταξύ των φορέων τυποποίησης και της αναπτυξιακής κοινότητας. Η ανάπτυξη νέων προτύπων ή η προσαρμογή των υπαρχόντων θα συμβάλει στην παροχή συνοχής στη διαχείριση ασφάλειας για την παγκόσμια αλυσίδα εφοδιασμού για IoT και στη βελτίωση της ενσωμάτωσης των πληροφοριών ασφαλείας σε όλους τους παράγοντες. Μία από τις σημαντικότερες προκλήσεις που σχετίζονται με αυτό το ζήτημα είναι η εξεύρεση δομικών στοιχείων για την αλυσίδα εφοδιασμού που είναι ουσιαστικά και γενικά αρκετά ώστε να εφαρμόζονται με οριζόντιο τρόπο, μειώνοντας έτσι το κόστος εισαγωγής ενός προτύπου για μικρές και μεσαίες εταιρείες. [26]
]

8.4.13 Παροχή λογισμικού υλικού (sboms) για συσκευές IoT

Ένα SBOM περιγράφει τα στοιχεία λογισμικού που χρησιμοποιούνται ως δομικά στοιχεία οποιουδήποτε δεδομένου προϊόντος με εξαντλητικό τρόπο, συμπεριλαμβανομένων τόσο των ανοιχτών πηγών όσο και των εμπορικών πακέτων ή βιβλιοθηκών. Αυτές οι λίστες αυξάνουν την ορατότητα στο προϊόν και επιτρέπουν τόσο στον κατασκευαστή όσο και στους εξωτερικούς χρήστες να ελέγχουν για γνωστά τρωτά σημεία και να επικυρώνουν τη συσκευή από άποψη ασφάλειας, συμβάλλοντας στη μείωση των κενών ευπάθειας που ενδέχεται να επιτρέψουν στους εισβολείς να αξιοποιήσουν επιτυχώς μια ευπάθεια για κακόβουλους σκοπούς. Η αυξημένη ορατότητα του προϊόντος μπορεί επίσης να οδηγήσει σε αύξηση εμπιστοσύνη μεταξύ των παραγόντων της αλυσίδας εφοδιασμού. Τα SBOMs θα πρέπει ιδανικά να είναι διαθέσιμα για όλα τα προϊόντα IoT οποιουδήποτε οργανισμού, ανεξάρτητα από το εάν διανέμονται στο εμπόριο ή όχι. Τα SBOM μπορούν να χρησιμεύσουν ως δομικό στοιχείο για την εφαρμογή ενός συστήματος διαχείρισης διαμόρφωσης και εκδόσεων. Αυτά τα συστήματα υποστηρίζουν την εξέλιξη των στοιχείων του λογισμικού, βελτιώνοντας την ιχνηλασιμότητα και επιτρέποντας στους χρήστες και τους οργανισμούς να καθορίσουν ένα χρονοδιάγραμμα των εκδόσεων λογισμικού. Αυτό, με τη σειρά του, μπορεί να χρησιμοποιηθεί για την επαναφορά σε προηγούμενες σταθερές καταστάσεις σε περίπτωση απροσδόκητων προβλημάτων. [26]

8.5 Τεχνολογίες για την διασφάλιση της ασφάλειας

8.5.1 Εγκατάσταση και βελτίωση σχεδιασμού και διαχείρισης της αναβάθμισης της συσκευής και παραβολής

Η ανάγκη εκσυγχρονισμού και βελτίωσης της ποιότητας και των λειτουργιών των συσκευών συνήθως οδηγεί σε λύσεις IoT όπου συνυπάρχουν αρκετές γενιές συσκευών και λογισμικού, οι οποίες πρέπει να ενημερωθούν ώστε να μην είναι ξεπερασμένες και να αποφεύγουν να αντιμετωπίζουν διαφορετικά επίπεδα ασφάλειας και ασφάλειας. Το πεδίο εφαρμογής της αλυσίδας εφοδιασμού πρέπει να επεκταθεί προς το τέλος της διάρκειας ζωής οποιασδήποτε συνδεδεμένης συσκευής, ειδικά εάν εμπλέκονται ενημερώσεις OTA. Η ενημέρωση των συσκευών IoT είναι δύσκολη, καθώς τα προϊόντα βασίζονται συνήθως σε διάφορα πακέτα από διαφορετικές πηγές και χρησιμοποιούν διαφορετικά εργαλεία και στοιχεία τρίτων. Ο σχεδιασμός και η διαχείριση αυτών των ενημερώσεων είναι κάτι πολύ σημαντικό να ληφθεί υπόψη. Οι αναδυόμενες τεχνολογίες θα μπορούσαν να βοηθήσουν στην προβολή της αλυσίδας εφοδιασμού για IoT και πρέπει τουλάχιστον να αξιολογηθούν. Οι οργανισμοί πρέπει πρώτα να εκτιμήσουν τη βιωσιμότητά τους από άποψη ασφάλειας πριν δεσμευτούν σε μια αίτηση. Παραδείγματα τέτοιων τεχνολογιών περιλαμβάνουν το Blockchain, το οποίο μπορεί να χρησιμοποιηθεί για την παροχή ισχυρών εγγυήσεων ακεραιότητας σε συστήματα ιχνηλασιμότητας. και τεχνητή νοημοσύνη (AI), που θα μπορούσαν να βοηθήσουν τους επαγγελματίες στη διαδικασία λήψης αποφάσεων για ένα ευρύ φάσμα θεμάτων. Για παράδειγμα, το Device Fingerprinting (DFP) είναι ένα παράδειγμα εφαρμογής του AI όπου η ταυτότητα της συσκευής προέρχεται από τη δραστηριότητα του δικτύου της χωρίς την ανάγκη ανάγνωσης μιας σαφούς ταυτότητας. Ωστόσο, οι οργανισμοί πρέπει να λαμβάνουν υπόψη το γεγονός ότι η τεχνητή νοημοσύνη δεν παρέχει απόλυτες εγγυήσεις απόδοσης και θα πρέπει να χρησιμοποιείται ως συμπληρωματικό εργαλείο σε σημαντικό αριθμό περιπτώσεων. [26]

8.5.2 Χρήση μηχανισμών υλικού για την παροχή Εσωτερικής επικύρωσης

Ενσωματώστε τεχνικές συσκότισης υλικού στις διαδικασίες σχεδιασμού κυκλώματος για προστασία από απειλές όπως η αντίστροφη μηχανική και η υπερπαραγωγή. Αυτές οι τεχνικές βασίζονται στην προσθήκη βασικών εισόδων που δεν είναι κρίσιμες για την πραγματική λειτουργικότητα του κυκλώματος, αλλά χρησιμοποιούνται για την επικύρωση της λειτουργίας. η έξοδος των εν λόγω κυκλωμάτων δεν θα ήταν σωστή παρουσία μη έγκυρου κλειδιού. Τα μυστικά κλειδιά δεν πρέπει να είναι γνωστά στα μη αξιόπιστα χυτήρια και OSAT και θα πρέπει να ενεργοποιηθούν αργότερα κατά τη διαδικασία κατασκευής από τον κάτοχο της IP. Με σχετικό τρόπο, τα κλειδιά μεταφοράς ή / και τα κλειδιά ενεργοποίησης θα πρέπει να χρησιμοποιούνται για την προστασία από κλοπή κατά τη μεταφορά [26]

8.5.3 Υπενθυμίζουν την έγκριση slas που ζητεί την παρουσία μέτρων ασφάλειας λογισμικού

Η ασφαλής υπογραφή εκκίνησης και υλικολογισμικού είναι μέτρα ασφαλείας που παρέχουν ένα βαθμό προστασίας έναντι παραβίασης. Σε περίπτωση υπογραφής υλικολογισμικού, ο κατακερματισμός οποιασδήποτε δεδομένης εικόνας υλικολογισμικού υπογράφεται χρησιμοποιώντας ένα ιδιωτικό κλειδί που είναι διαθέσιμο μόνο στον γνήσιο πάροχο του λογισμικού Το δημόσιο κλειδί χρησιμοποιείται αργότερα από τη συσκευή για την επαλήθευση της ακεραιότητας των εικόνων υλικολογισμικού. Η ασφαλής εκκίνηση αναφέρεται στην πρακτική της κρυπτογραφικής επικύρωσης ολόκληρης της αλυσίδας στοιχείων λογισμικού που συμμετέχουν στη διαδικασία εκκίνησης της συσκευής ξεκινώντας από μια αμετάβλητη ρίζα εμπιστοσύνης. Αυτά τα μέτρα ακεραιότητας πρέπει να χρησιμοποιούνται κατά την κατασκευή συσκευών (όταν το υλικολογισμικό αναβοσβήνει κατά την πρώτη εκκίνηση) και κατά τη συντήρηση (σε OTA) αυτές οι κρυπτογραφικές λειτουργίες πρέπει να γίνονται σε συνδυασμό με ένα ανθεκτικό σε παραβίαση υλικό στο πλαίσιο της αλυσίδας εμπιστοσύνης (που είναι η παραβίαση ανθεκτικό υλικό η ρίζα). Αυτά τα δύο μέτρα μπορούν να ενσωματωθούν σε υπάρχουσες συμφωνίες επιπέδου υπηρεσίας με τρίτους προμηθευτές. Αξίζει επίσης να σημειωθεί ότι τα μέλη της GlobalPlatform εργάζονται για την ανάπτυξη προτύπων ασφαλείας που ορίζουν μια σειρά θεμελίων ασφαλείας (SRF) (π.χ. root of trust, ασφαλής εγκατάσταση υλικολογισμικού) - αυτά θα μπορούσαν να χρησιμοποιηθούν για να παρέχουν ορατότητα των δυνατοτήτων ασφαλείας στα chip. Αυτά τα μέτρα ακεραιότητας πρέπει να χρησιμοποιούνται κατά την κατασκευή της συσκευής (όταν το υλικολογισμικό αναβοσβήνει κατά την πρώτη εκκίνηση) και κατά τη συντήρηση (σε OTA). ii) αυτές οι κρυπτογραφικές λειτουργίες πρέπει να γίνονται σε συνδυασμό με ένα ανθεκτικό σε παραβίαση υλικό στο πλαίσιο της αλυσίδας εμπιστοσύνης (ως το ανθεκτικό σε παραβίαση υλικό η ρίζα). [26]

8.5.4 Συστήματα διαχείρισης ολοκληρωμένης ταυτότητας για συσκευές IoT

Η ικανότητα μοναδικής αναγνώρισης κάθε συσκευής IoT είναι ζωτικής σημασίας και έχει βαθιές επιπτώσεις που σχετίζονται με την ορατότητα και την υπευθυνότητα στην αλυσίδα εφοδιασμού. Τα συστήματα διαχείρισης ταυτότητας πρέπει να ενσωματωθούν στην αλυσίδα εφοδιασμού για να παρέχουν αυτά τα μοναδικά αναγνωριστικά. Περιλαμβάνονται συνήθως στο ευρύτερο πλαίσιο των συστημάτων διαχείρισης ταυτότητας και πρόσβασης (IAM) που ρυθμίζουν τον κύκλο ζωής της ταυτότητας της συσκευής και παρέχουν υπηρεσίες ελέγχου ταυτότητας και εξουσιοδότησης. [26]

8.5.5 Ολοκληρώστε μια δυνατό ριζά εμπιστοσύνης

Μια ρίζα εμπιστοσύνης είναι το πρώτο στοιχείο της αλυσίδας εμπιστοσύνης μιας συσκευής. Συνήθως υλοποιείται χρησιμοποιώντας ένα εξειδικευμένο στοιχείο υλικού που παρέχει ένα σύνολο κρυπτογραφικών δυνατοτήτων και πρωτόγονων που μπορούν να θεωρηθούν

αξιόπιστα από τη συσκευή. Αυτά τα στοιχεία είναι συνήθως ανθεκτικά σε παραβίαση σε επίπεδο υλικού και μπορούν να χρησιμοποιηθούν ως βάση για μέτρα ασφαλείας, όπως υπογραφή υλικολογισμικού ή ασφαλής εκκίνηση. Υπάρχουν επίσης εναλλακτικές λύσεις λογισμικού με χαμηλότερο κόστος, αν και είναι πολύ πιο ευάλωτες, και επομένως, εν γένει, είναι κατάλληλες για περιορισμένο εύρος εφαρμογών. Οι παράγοντες της αλυσίδας εφοδιασμού IoT (π.χ. πάροχοι λειτουργικών συστημάτων, προγραμματιστές εφαρμογών) θα πρέπει να βασίζουν τις συνεισφορές τους σε αυτό το ίδρυμα ασφαλείας, όταν είναι δυνατόν. [26]

8.5.6 Μηχανισμοί εφαρμογής για την αποκατάσταση ενημέρωσης

Η δυνατότητα εφαρμογής ενημερώσεων με απομακρυσμένο και αυτοματοποιημένο τρόπο για συσκευές στο πεδίο είναι καθοριστικής σημασίας για τη διαδικασία ασφάλειας για την αλυσίδα εφοδιασμού. Τα στάδια του κύκλου ζωής Οι περισσότερες συσκευές IoT δεν είναι διακριτές, δηλαδή μπορεί να προκύψει περαιτέρω ανάπτυξη μετά την ανάπτυξη της συσκευής. και ευπάθειες με αντίκτυπο στα συστήματα της εφοδιαστικής αλυσίδας μπορούν να ανακαλυφθούν αργότερα ή ως αποτέλεσμα των δεδομένων που συλλέγονται από μια πραγματική επίθεση. Η ικανότητα ταχείας αντίδρασης σε αλλαγές στο περιβάλλον και η ανάπτυξη ενημερώσεων για απομακρυσμένες συσκευές πρέπει να συμπεριλαμβάνεται και να λαμβάνεται υπόψη από τα προηγούμενα στάδια του σχεδιασμού. Επιπλέον, αυτοί οι μηχανισμοί πρέπει να είναι ασφαλείς για την αποτροπή κακής χρήσης και ένεσης κακόβουλου λογισμικού. [26]

8.5.7 ολοκληρωμένοι μηχανισμοί αδείας σε κυκλώματα

Για την υποστήριξη της ανιχνευσιμότητας και της συντήρησης, ο έλεγχος ταυτότητας συσκευής είναι υποχρεωτικός. Physical Unclonable Functions (PUF) - ένα πρωτόγονο με βάση τα φυσικά χαρακτηριστικά ενός κυκλώματος που προέρχεται από τη διαδικασία κατασκευής του και παρέχει σαφή αναγνώριση - είναι μια από τις πιο σημαντικές διαθέσιμες επιλογές. Αυτό σημαίνει ότι το PUF μπορεί να χρησιμοποιηθεί για να προσδιορίσει εάν μια δεδομένη συσκευή είναι γνήσια, βελτιώνοντας την ιχνηλασιμότητα των συσκευών σε όλη την αλυσίδα εφοδιασμού. Τα πλεονεκτήματα του PUF περιλαμβάνουν αντίσταση σε επεμβατικές επιθέσεις, οι οποίες απαιτούν από τον εισβολέα να αντιμετωπίσει την περίπλοκη προοπτική τροποποίησης των φυσικών χαρακτηριστικών του κυκλώματος. Πρέπει να σημειωθεί ότι, εκτός από το PUF, μπορούν να χρησιμοποιηθούν και άλλες τεχνολογίες όπως το Trusted Execution Environments (TEE). Συνδέεται στενά με αυτήν την καλή πρακτική είναι η σύσταση σωστής αξιοποίησης των δεδομένων ιχνηλασιμότητας που ενδέχεται να περιλαμβάνονται ήδη από τους κατασκευαστές πυριτίου στα τσιπ τους. [26]

8.5.8 Εξέταση των δυνατοτήτων cybersecurity εισαγωγή με συνεργασία λογισμικού υλικού

Τα προγράμματα συνεργασίας υλικού-λογισμικού είναι μια προσέγγιση που επικεντρώνεται στην κάλυψη του κενού ασφάλειας στον κυβερνοχώρο που αφήνει τα μέτρα ασφαλείας που λειτουργούν αποκλειστικά στα επίπεδα υλικού ή λογισμικού. Τα μέτρα υλικού μπορούν να επωφεληθούν από το πλαίσιο που παρέχεται από την τρέχουσα κατάσταση του συστήματος σε επίπεδο λογισμικού. ενώ οι ευπάθειες στα μέτρα λογισμικού μπορούν να καλυφθούν όταν το λογισμικό είναι σε θέση να επικοινωνεί με εξειδικευμένα στοιχεία υλικού, ειδικά σε εκείνες τις περιπτώσεις όπου ο εισβολέας αποκτά προνομιακή πρόσβαση / root. Θα μπορούσε να υποστηριχθεί ότι η αξιόπιστη εκτέλεση μπορεί να επιτευχθεί μόνο με το συνδυασμό υλικού και λογισμικού. Παραδείγματα εφαρμογών αυτών των συστημάτων περιλαμβάνουν ασφαλή αποθήκευση για κλειδιά που βασίζονται σε PUF και εγγυήσεις ασφαλείας για μη αξιόπιστες επεκτάσεις πυρήνα. Η ασφάλεια των συσκευών IoT μπορεί να βελτιωθεί σημαντικά εφαρμόζοντας αυτά τα σχήματα σε περιπτώσεις όπου είναι εφικτό, ωστόσο, αυτό είναι συνήθως μια προσπάθεια που απαιτεί υψηλή τεχνική εμπειρογνωμοσύνη. [26]

9 Δοκιμές διείσδυσης (Penetration Test)

9.1 Για τις δοκιμές διείσδυσης θα χρησιμοποιήσουμε τα παρακάτω:

- Έναν φορητό υπολογιστή Dell με επεξεργαστή
  Intel (R) Core (TM) i5-6300U CPU @ 2.40GHz 2.50GHz
  Εγκατεστημένη μνήμη RAM 8GB
  Windows 10 Pro 64 bit

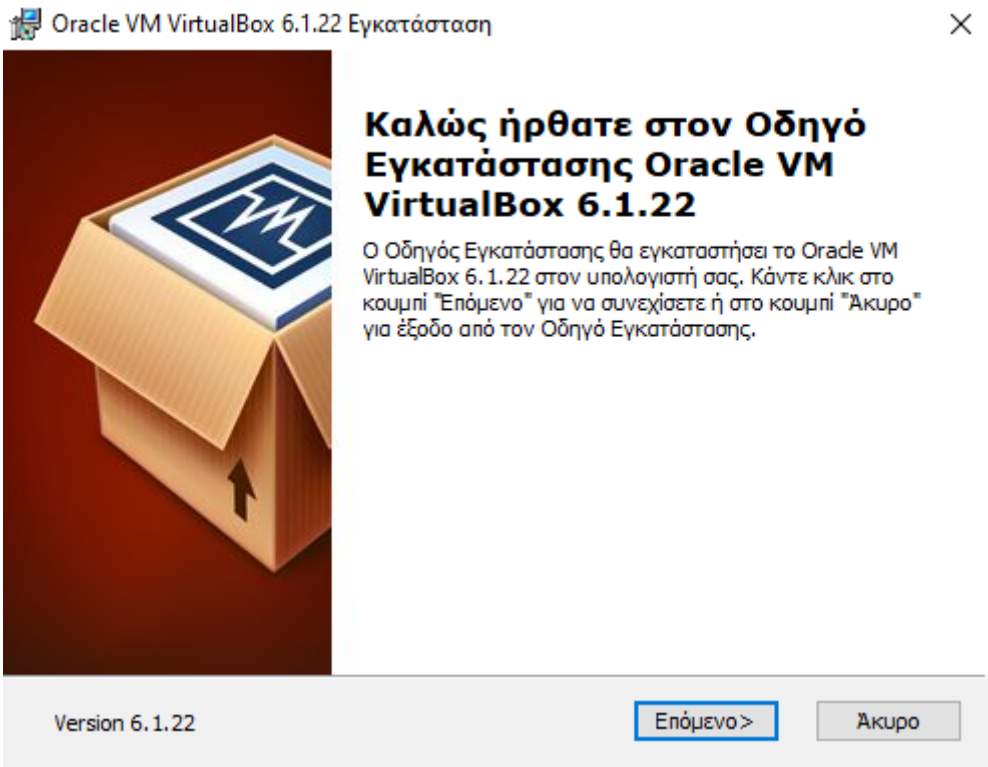
- Θα χρησιμοποιήσουμε το Oracle VM VirtualBox, ένα πρόγραμμα εικονικοποίησης x86 και AMD64 / Intel64.Το VirtualBox διατίθεται ελεύθερα ως λογισμικό ανοιχτού κώδικα υπό τους όρους της έκδοσης 2. GNU General Public License (GPL). Και εκτελείται σε κεντρικούς υπολογιστές Windows, Linux, Macintosh και Solaris και υποστηρίζει μεγάλο αριθμό λειτουργικών συστημάτων επισκεπτών, συμπεριλαμβανομένων ενδεικτικά των Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS / Windows 3.x, Linux (2.4, 2.6, 3.x και 4.x), Solaris και OpenSolaris, OS / 2 και OpenBSD. Το VirtualBox αναπτύσσεται ενεργά με συχνές εκδόσεις και διαθέτει μια συνεχώς αυξανόμενη λίστα χαρακτηριστικών, υποστηριζόμενων λειτουργικών συστημάτων και πλατφορμών για τους οποίους λειτουργεί.

- Θα χρησιμοποιήσουμε το λειτουργικό Kali Linux που είναι μια διανομή Linux ανοιχτού κώδικα, βασισμένη στο Debian, προσανατολισμένη σε διάφορες εργασίες ασφάλειας πληροφοριών, όπως Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

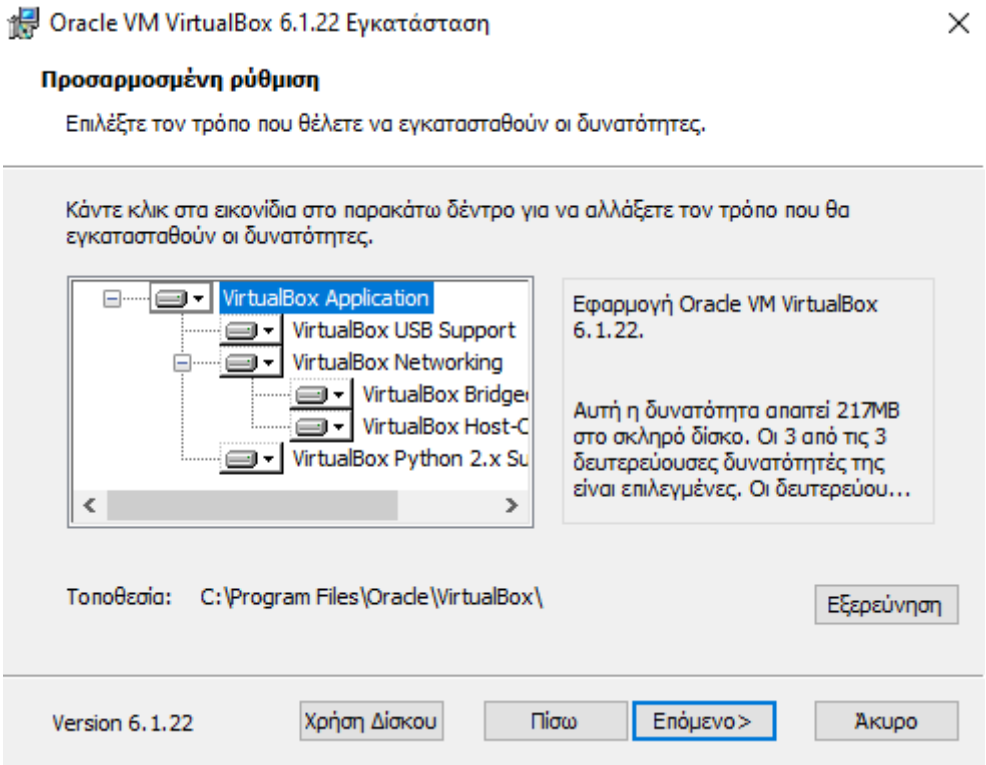
- Θα χρησιμοποιήσουμε το OWASP BWA που είναι μία ευάλωτη εικονική μηχανή και φιλοξενείται στο SourceForge, ένα δημοφιλές αποθετήριο για έργα ανοιχτού κώδικα.

9.2 Εγκατάσταση λογισμικού Oracle VM VirtualBox

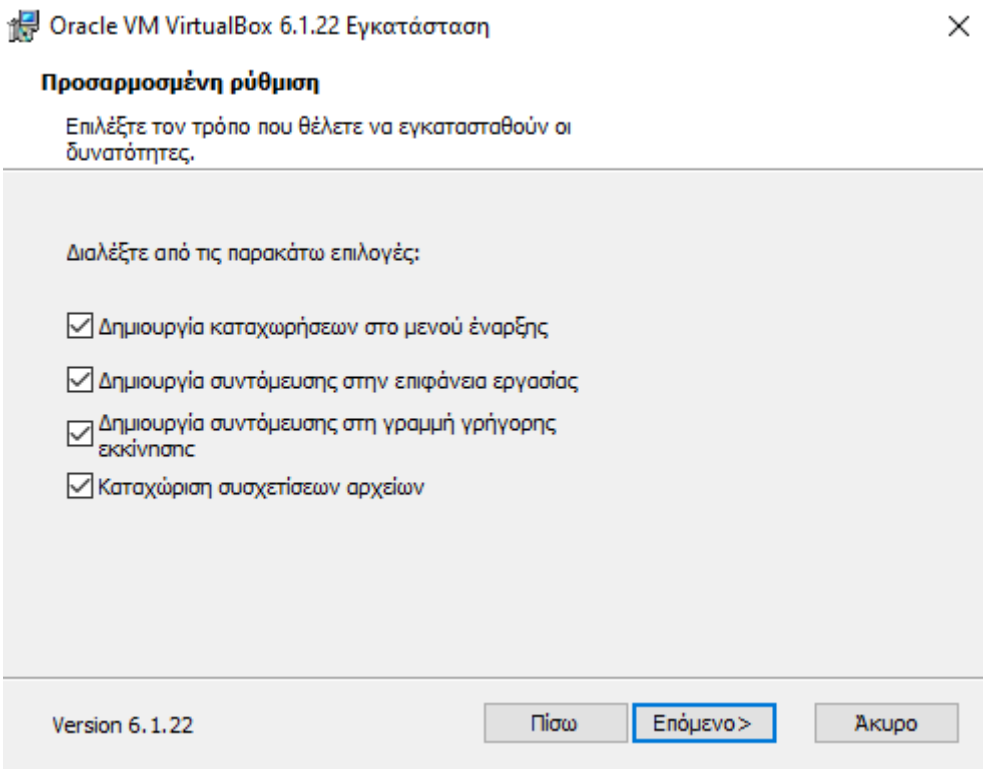
Για να κάνουμε εγκατάσταση το Oracle VM VirtualBox επισκεπτόμαστε την σελίδα https://www.virtualbox.org/wiki/Downloads και στο πεδίο VirtualBox 6.1.22 platform packages επιλέγουμε Windows hosts και κατεβάζουμε το VirtualBox-6.1.22-144080.exe αρχείο και το κάνουμε εγκατάσταση όπως φαίνεται στις εικόνες που ακολουθούν.



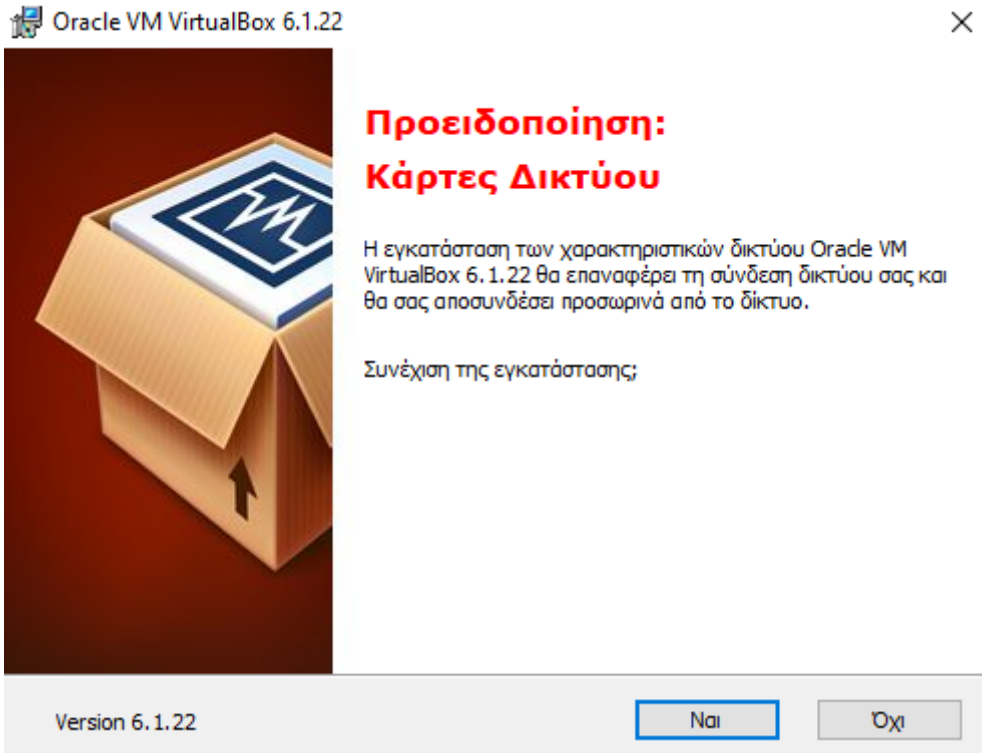
Εικόνα 18 Εγκατάσταση VM Virtual Box πατάμε Επόμενο



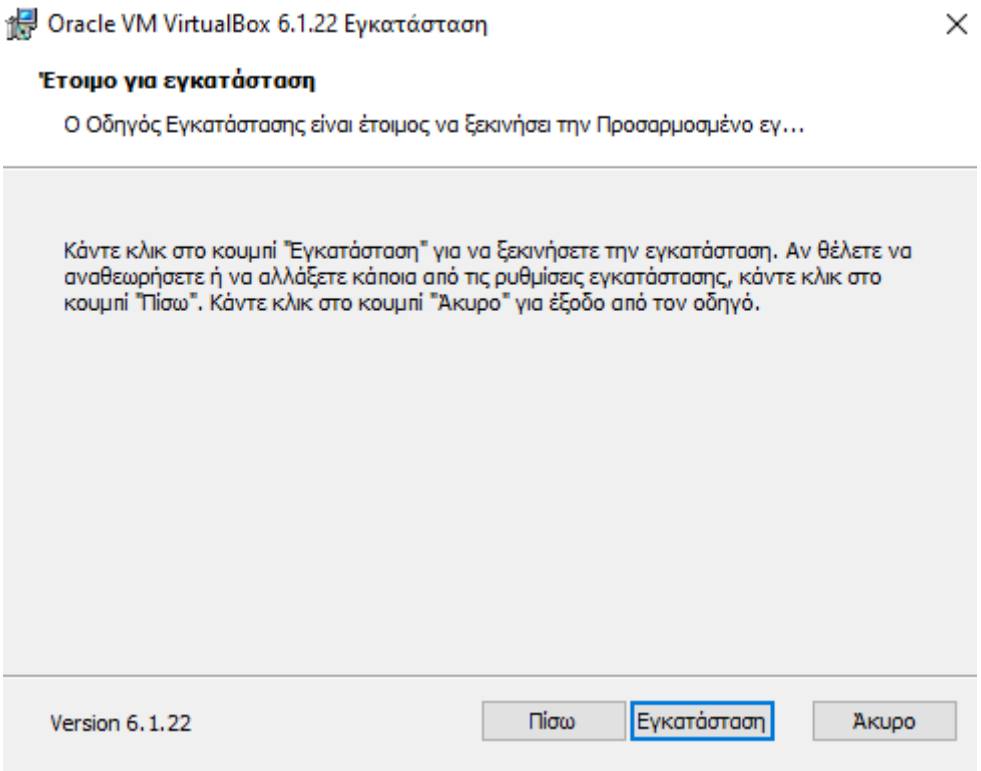
Εικόνα 19 Εγκατάσταση VM Virtual Box πατάμε Επόμενο



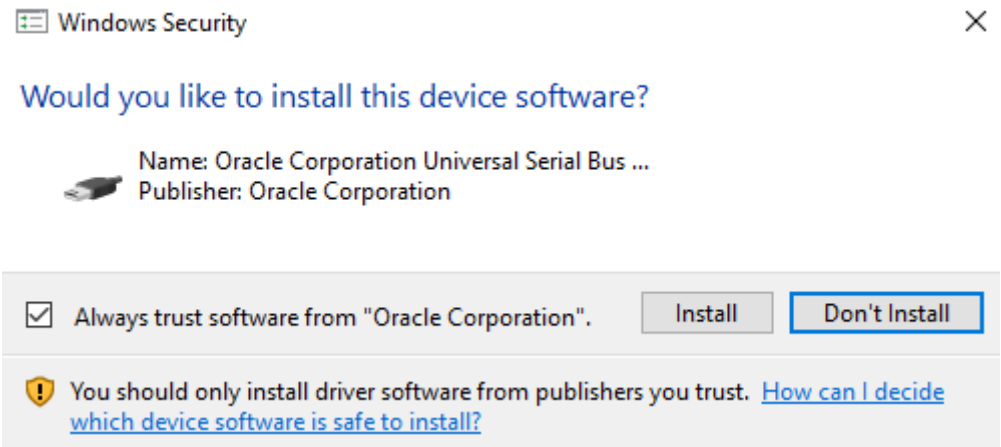
Εικόνα 20 Εγκατάσταση VM Virtual Box πατάμε Επόμενο



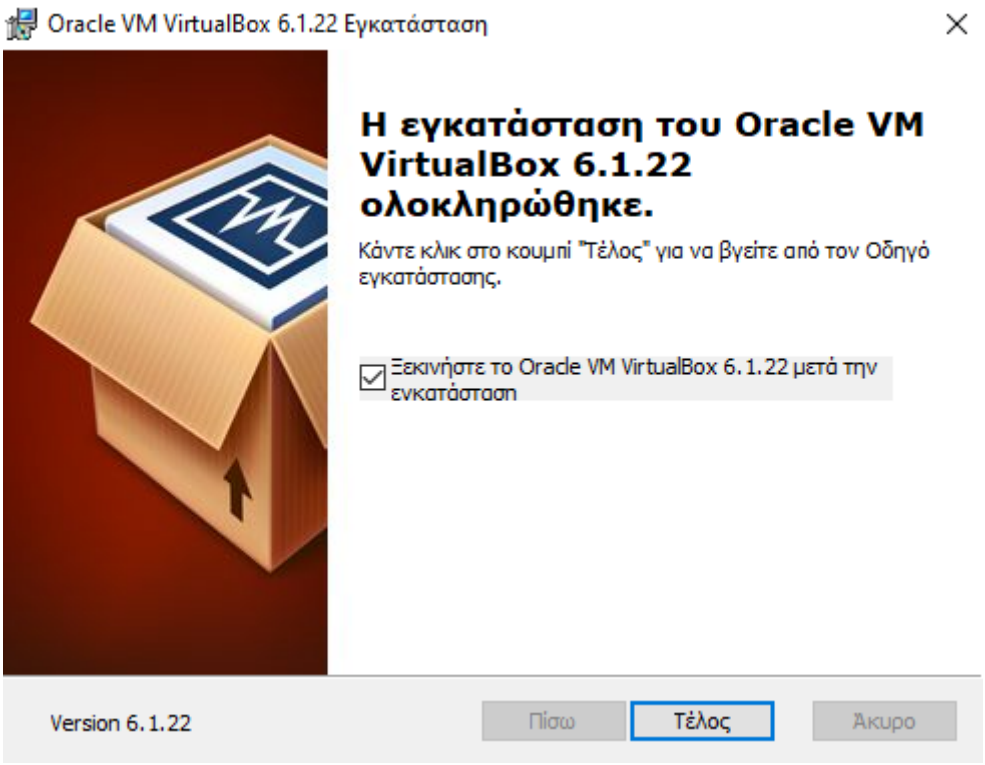
Εικόνα 21 Εγκατάσταση VM Virtual Box πατάμε Ναι



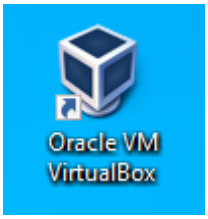
Εικόνα 22 Εγκατάσταση VM Virtual Box πατάμε Εγκατάσταση



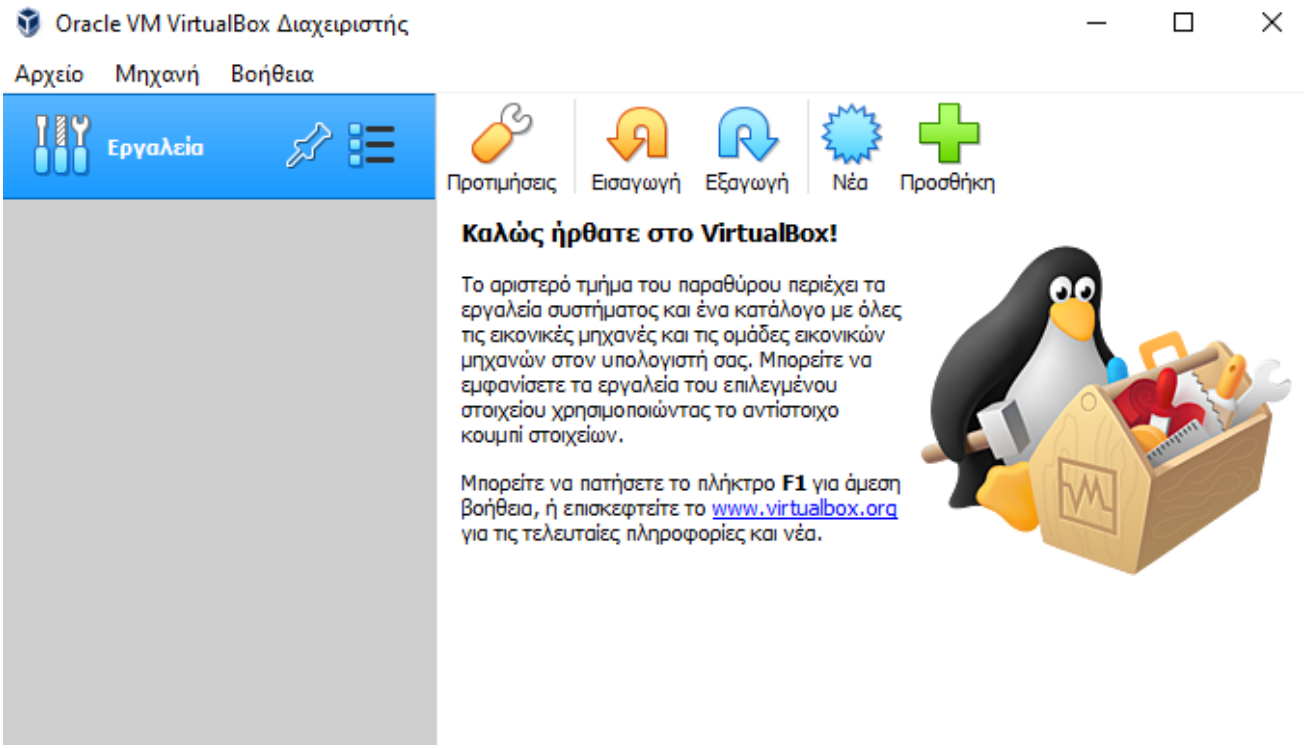
Εικόνα 23 Εγκατάσταση VM Virtual Box πατάμε Install



Εικόνα 24 Εγκατάσταση VM Virtual Box πατάμε Τέλος



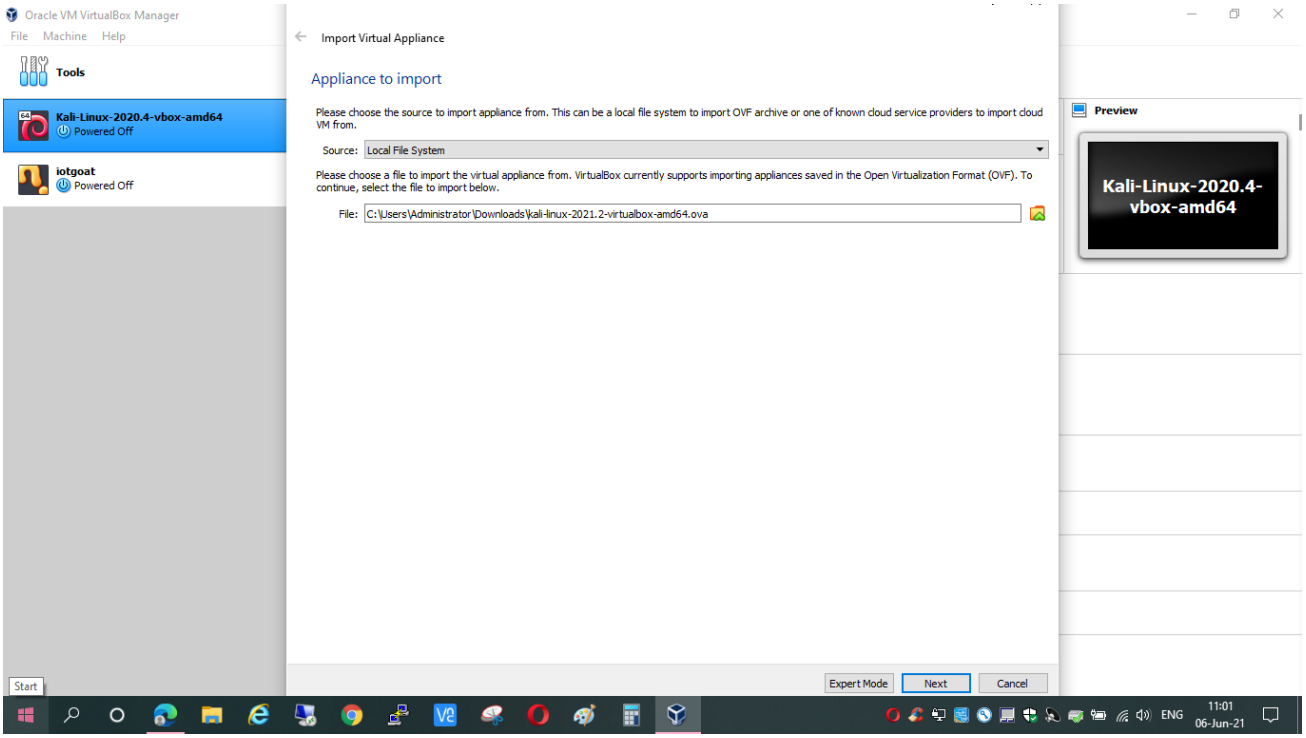
Εικόνα 25 Συντόμευση στην Επιφάνεια Εργασίας



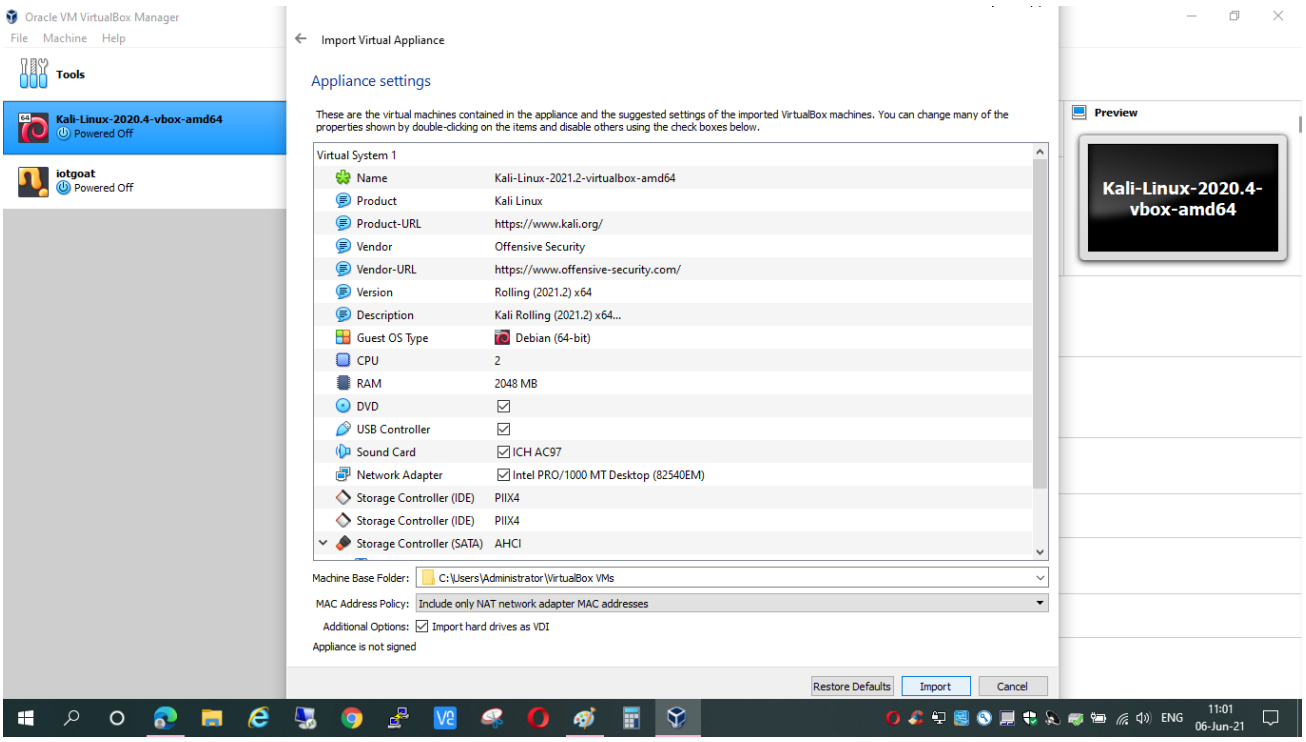
Εικόνα 26 Άνοιγμα εφαρμογής VM VirtualBox

9.3 Εγκατάσταση λειτουργικού Kali Linux στο VM VirtualBox

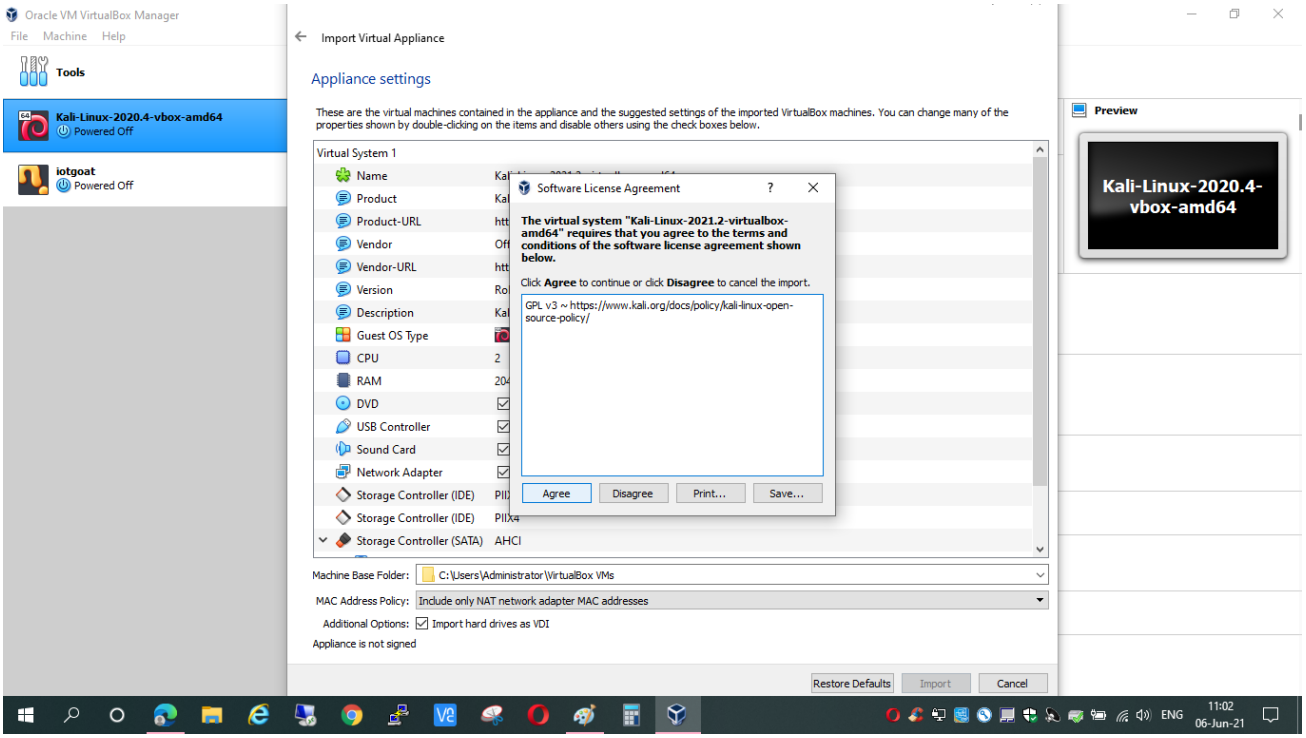
Για να κάνουμε εγκατάσταση το Kali Linux στο VirtualBox επισκεπτόμαστε την σελίδα https://www.kali.org/ επιλέγουμε Download μετά Virtual Machines και κάνουμε Download το λογισμικό Kali Linux για το VM VirtualBox στα 64bit ή στα 32bit ανάλογα με το λειτουργικό μας, στο παράδειγμά μας είναι Windows 64bit. Το αρχείο που κατεβάσαμε είναι το kali-linux-2021.2-virtualbox-amd64.ova και από το πρόγραμμα VirtualBox όπως φαίνεται στην εικόνα 26 επιλέγουμε το Αρχείο μετά Εισαγωγή Συσκευής και επιλέγουμε το path που είναι το αρχείο kali-linux-2021.2-virtualbox-amd64.ova και πατάμε το επόμενο όπως φαίνεται στην εικόνα 27 και ακολουθούμε τα βήματα που απεικονίζονται στις φωτογραφίες 28-30.



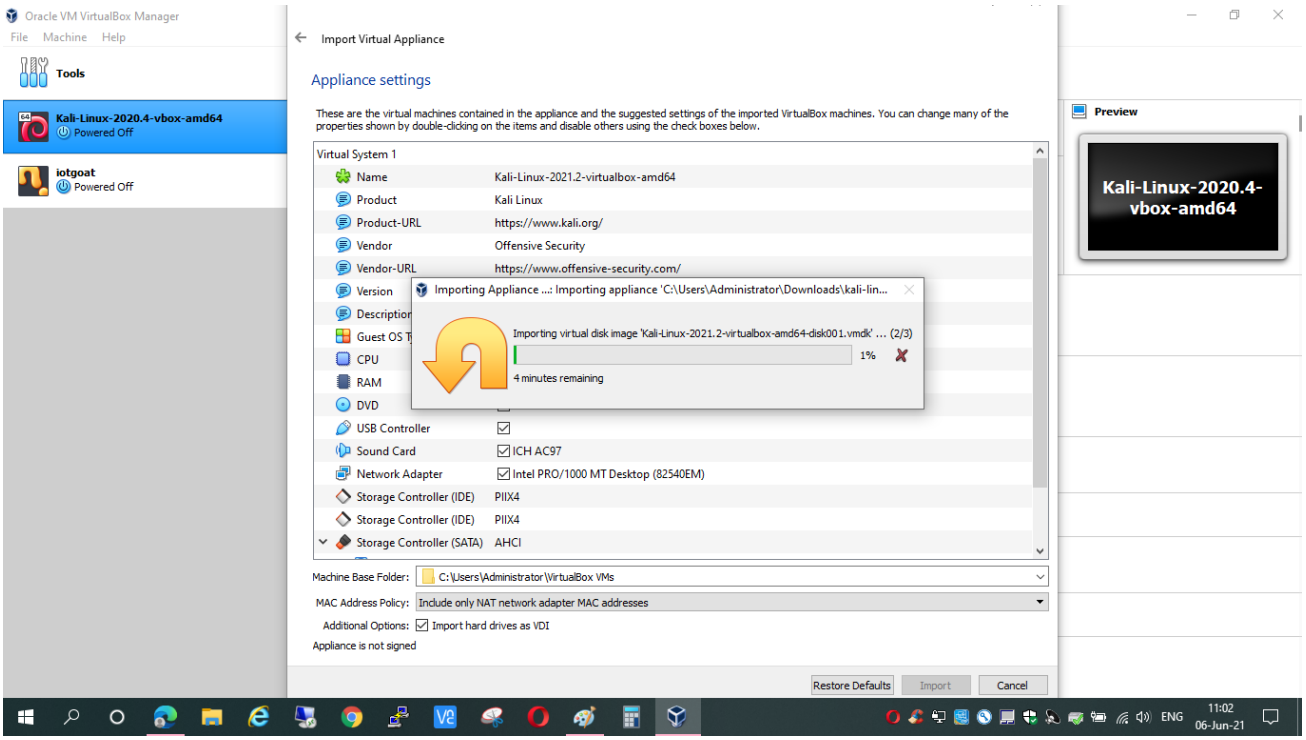
Εικόνα 27 Εισαγωγή Συσκευής kali-linux-2021.2-virtualbox-amd64



Εικόνα 28 Πατάμε Import για Εισαγωγή Συσκευής kali-linux-2021.2-virtualbox-amd64

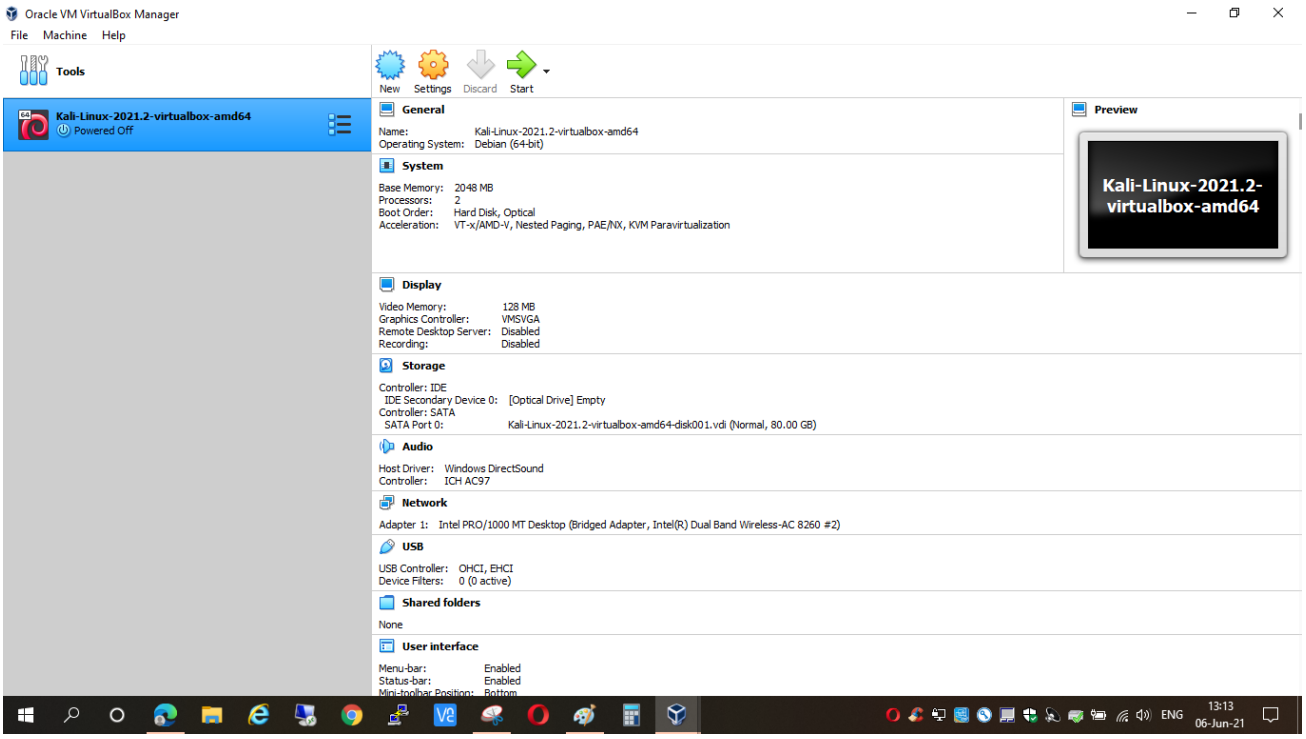


Εικόνα 29 Πατάμε Agree για Εισαγωγή Συσκευής kali-linux-2021.2-virtualbox-amd64

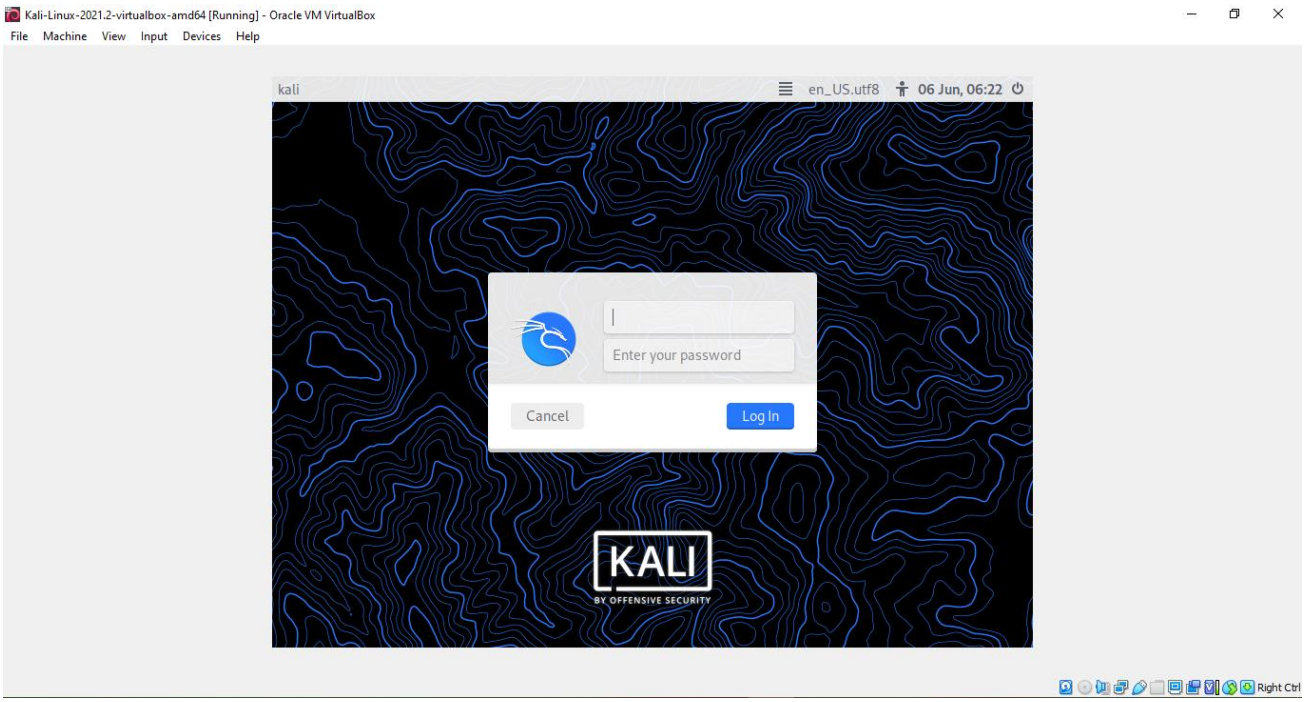


Εικόνα 30 Γίνεται Εισαγωγή Συσκευής kali-linux-2021.2-virtualbox-amd64

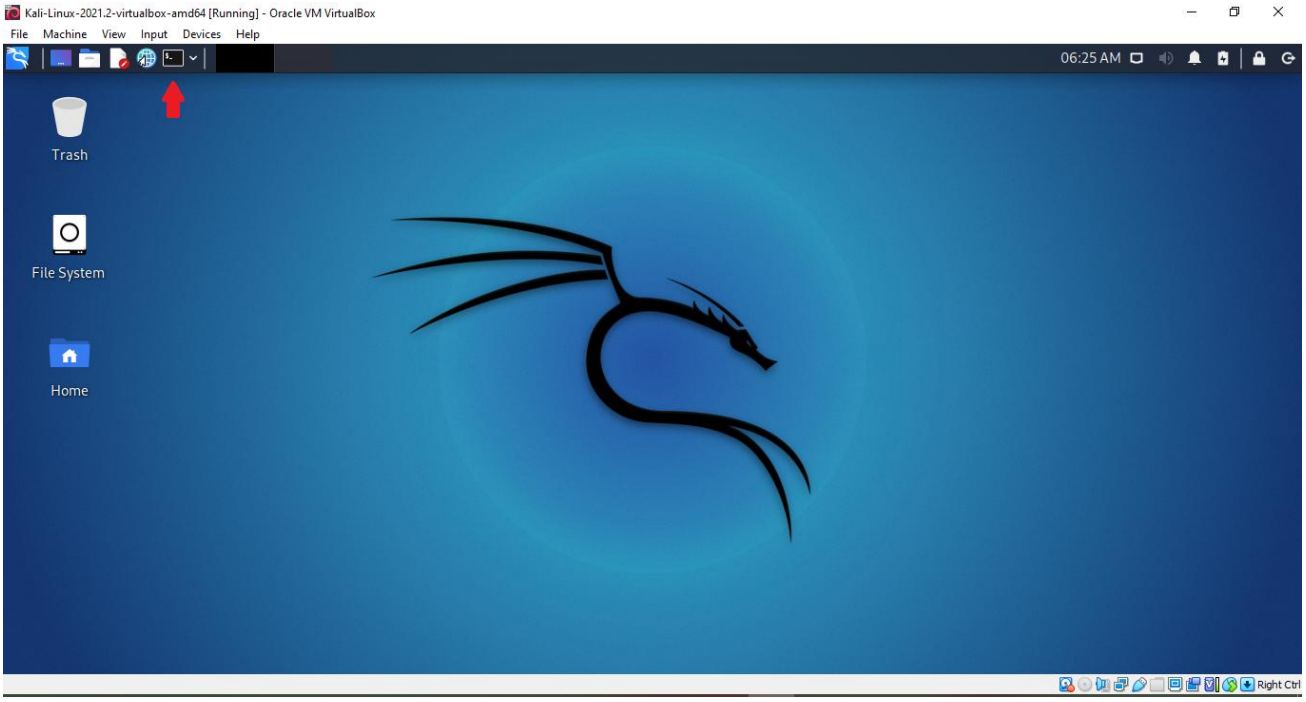
Αφού έχει γίνει η εισαγωγή της συσκευής kali-linux-2021.2-virtualbox-amd64 στο Oracle VM VirtualBox Manager όταν ξεκινάμε το πρόγραμμα επιλέγουμε την συσκευή και πατάμε start όπως φαίνεται στην εικόνα 31.



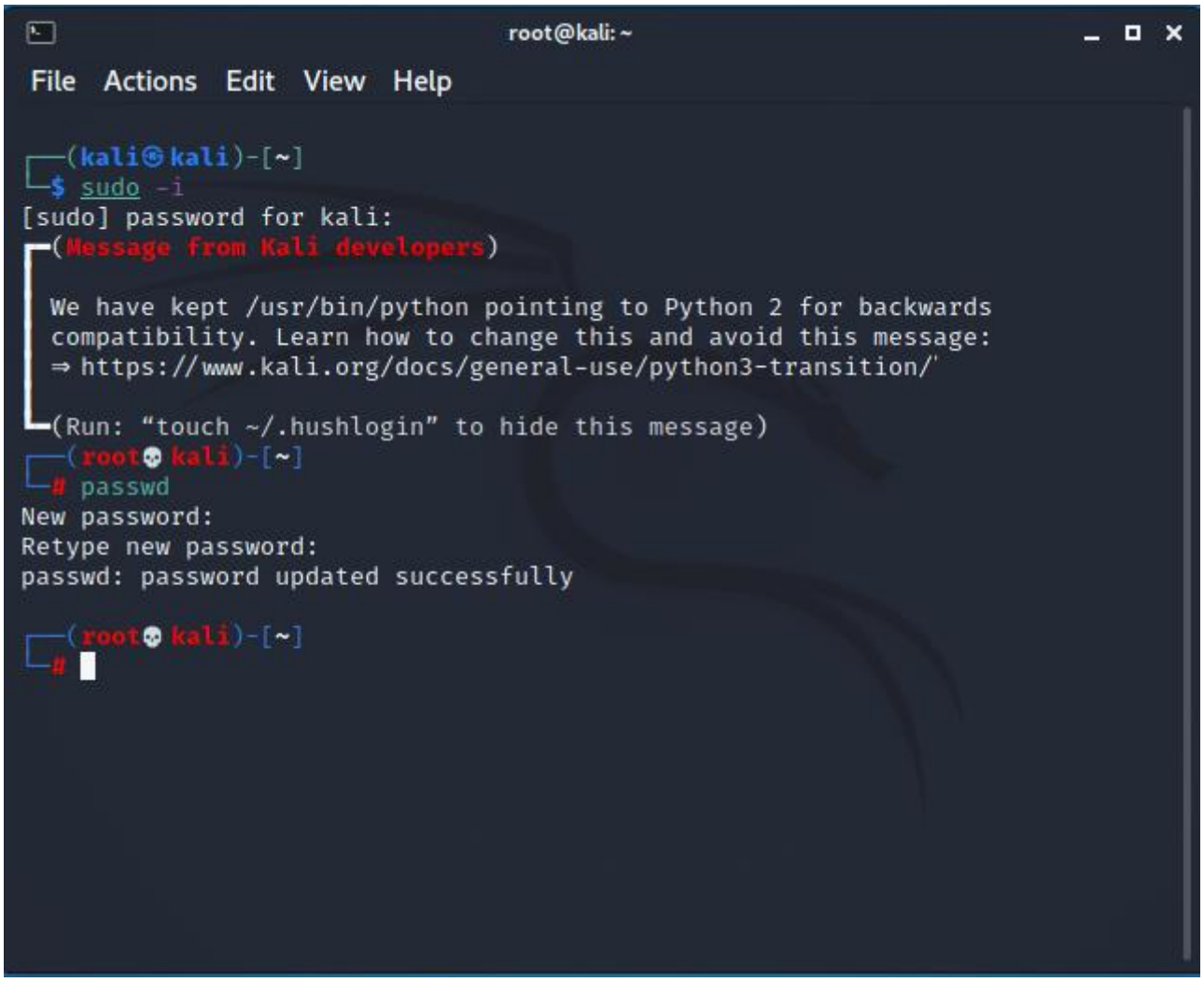
Εικόνα 31 Εκκίνηση συσκευής kali-linux-2021.2-virtualbox-amd64 στο VirtualBox



Εικόνα 32 Κάνουμε log in με τον χρήστη kali με κωδικό kali



Εικόνα 33 Άνοιγμα Terminal Emulator (κόκκινο βέλος)

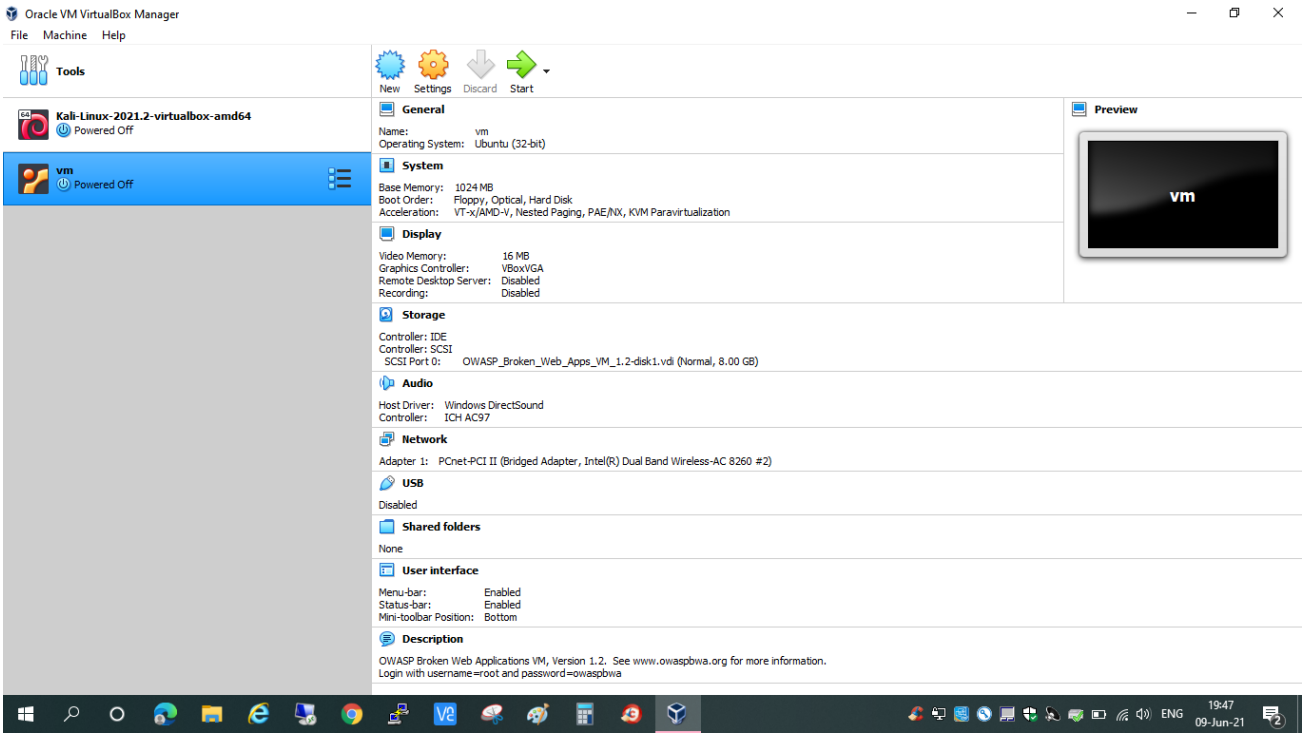


Εικόνα 34 Ενεργοποίηση κωδικού root

Ανοίγοντας το τερματικό εντολών του Kali Linux εκτελούμε την εντολή sudo-i εισάγουμε τον κωδικό του χρήστη Kali και μετά εκτελούμε την εντολή passwd εισάγουμε το νέο password και επαναπληκτρολογούμε το password για επαλήθευση, ο root είναι ενεργοποιημένος όπως φαίνεται στην εικόνα 34.

9.4 Εγκατάσταση OWASP BWA ευάλωτης εικονικής μηχανής

Στην σελίδα https://sourceforge.net/projects/owaspbwa/ κατεβάζουμε το αρχείο Released/1.2/OWASP_Broken_Web_Apps_VM_1.2.ova και το κάνουμε εισαγωγή συσκευής όπως και το kali-linux-2021.2-virtualbox-amd64 στις εικόνες 27 και 28. Ανοίγουμε από το VM VirtualBox την VM μηχανή και κάνουμε login στο OWASP BWA, ο χρήστης είναι root και ο κωδικός owaspbwa. Επίσης θα πρέπει να ρυθμίσουμε ώστε να είναι στο ίδιο δίκτυο οι δύο συσκευές στο VM VirtualBox για να επικοινωνούν.



Εικόνα 35 Εγκατάσταση ευάλωτης εικονικής μηχανής OWASP BWA

vm [Running] - Oracle VM VirtualBox

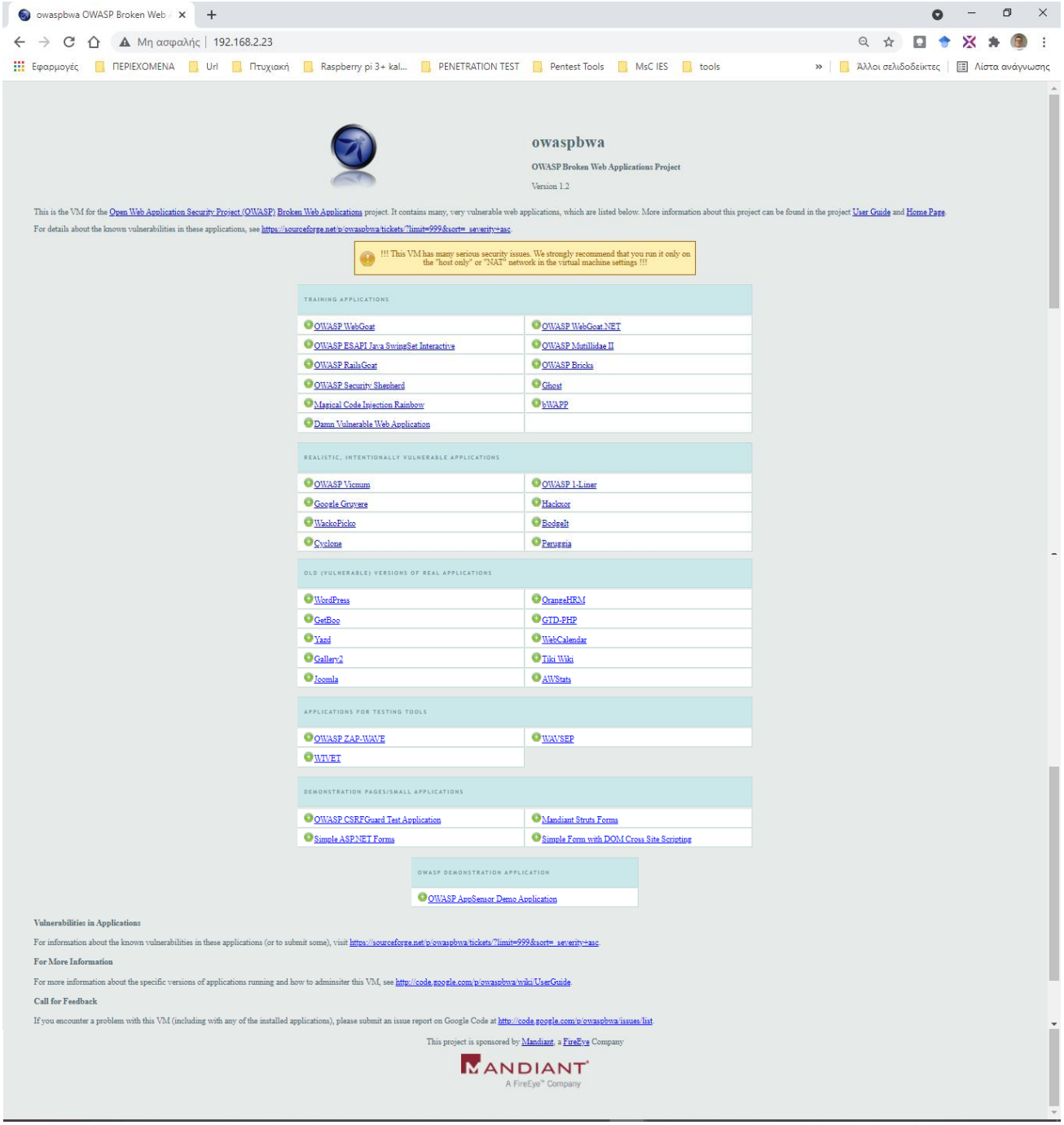
```
You can access the web apps at http://192.168.2.23/

You can administer / configure this machine through the console here, by SSHing
to 192.168.2.23, via Samba at \\192.168.2.23\, or via phpmyadmin at
http://192.168.2.23/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
Last login: Tue Jun  8 12:43:24 EDT 2021 on tty1
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.2.23/

You can administer / configure this machine through the console here, by SSHing
to 192.168.2.23, via Samba at \\192.168.2.23\, or via phpmyadmin at
http://192.168.2.23/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~#
```

Εικόνα 36 Εισαγωγή Username – Password

vm [Running] - Oracle VM VirtualBox

```
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:12:37:3a
          inet addr:192.168.2.23  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe12:373a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:544 errors:0 dropped:0 overruns:0 frame:0
          TX packets:220 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:53278 (53.2 KB)  TX bytes:133448 (133.4 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14673 (14.6 KB)  TX bytes:14673 (14.6 KB)

root@owaspbwa:~# _
```

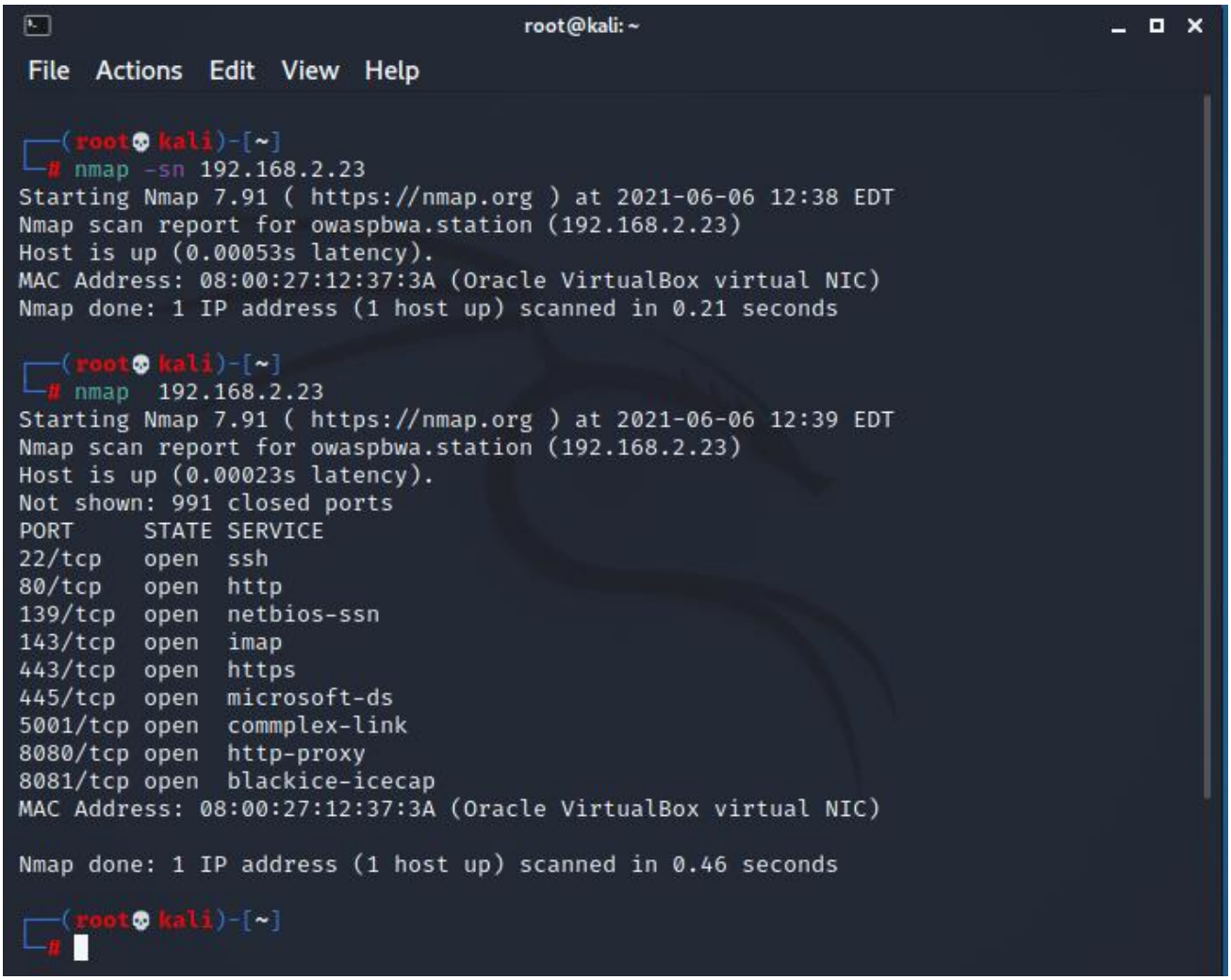
Εικόνα 37 Εντολή ifconfig



Εικόνα 38 Εφαρμογές διακομιστή OWASPBWA

9.5 Scanning and identifying services with nmap

Για να δούμε αν ο διακομιστής απαντά σε ping ή αν ο κεντρικός υπολογιστής είναι ενεργοποιημένος εκτελούμε την εντολή nmap -sn 192.168.2.23. Για να δούμε ποιες πόρτες είναι ανοιχτές και εκτελούμε την εντολή nmap 192.168.2.23 όπως φαίνεται στην εικόνα 39. Με την εντολή nmap -sV -O 192.168.56.11 βρίσκουμε τις εκδόσεις των υπηρεσιών που εκτελεί και το λειτουργικό σύστημα όπως φαίνεται στην εικόνα 40.



Εικόνα 39 Εντολή nmap και nmap –sn

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# nmap -sV -O 192.168.2.23                                          255 ✗
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 12:43 EDT
Nmap scan report for owaspbwa (192.168.2.23)
Host is up (0.00064s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0
)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1u
buntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/
2.2.14 OpenSSL ... )
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/https?
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, plea
se submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
SF-Port5001-TCP:V=7.91%I=7%D=6/6%Time=60BCFB44%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4,"\xac\xed\0\x05");
MAC Address: 08:00:27:12:37:3A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
```

Εικόνα 40 nmap -sV -O 192.168.2.23

Η εντολή Nmap περιλαμβάνει μερικά σενάρια για να γίνει έλεγχος WAF (τείχους προστασίας εφαρμογών ιστού) σε όλες τις HTTP θύρες που εντοπίστηκαν. Ένα τείχος προστασίας εφαρμογών ιστού (WAF) είναι μια συσκευή ή ένα λογισμικό που ελέγχει πακέτα που αποστέλλονται σε διακομιστή ιστού για να εντοπίζει και να αποκλείει αυτά που ενδέχεται να είναι κακόβουλα, συνήθως με βάση υπογραφές. Κατά τη διενέργεια δοκιμής διείσδυσης, η φάση αναγνώρισης πρέπει να περιλαμβάνει την ανίχνευση και ταυτοποίηση ενός WAF, intrusion detection system (IDS), or an intrusion prevention system (IPS). Είναι φανερό ότι δεν έχουμε WAF προστασία, όπως φαίνεται στην εικόνα 41.

```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root💀 kali)-[~]
└─# nmap -sT -sV -p80,443,8080,8081 --script http-waf-detect 192.168.2.23
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 12:55 EDT
Nmap scan report for owaspbwa (192.168.2.23)
Host is up (0.00047s latency).

PORT     STATE SERVICE    VERSION
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.
30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSS
L ... )
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suh
osin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Ph
usion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
443/tcp  open  ssl/https?
8080/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
8081/tcp open  http       Jetty 6.1.25
|_http-server-header: Jetty(6.1.25)
MAC Address: 08:00:27:12:37:3A (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds

┌──(root💀 kali)-[~]
└─#
```

Εικόνα 41 nmap -sT –sV χωρίς WAF προστασία

9.6 Προσδιορισμός κρυπτογράφησης HTTPS

Είναι συνηθισμένο να υποθέτουμε ότι όταν μια σύνδεση χρησιμοποιεί HTTPS με κρυπτογράφηση SSL ή TLS, είναι ασφαλής και κάθε εισβολέας που την αναχαιτίζει θα λάβει μόνο μια σειρά από αριθμούς χωρίς νόημα, χωρίς να είναι απόλυτα σωστό. Οι διακομιστές πρέπει να ρυθμιστούν σωστά ώστε να παρέχουν ένα ισχυρό επίπεδο κρυπτογράφησης και προστασία των χρηστών από επιθέσεις man-in-the-middle (MITM) ή κρυπτοανάλυση. Υπήρξαν ευπάθειες στην εφαρμογή και το σχεδιασμό του πρωτοκόλλου SSL και ανακαλύφθηκε ο διάδοχός του, TLS, που και αυτός έχει επίσης βρεθεί ότι είναι ευάλωτος σε ορισμένες διαμορφώσεις, καθιστώντας έτσι υποχρεωτική τη δοκιμή ασφαλών συνδέσεων σε οποιονδήποτε ιστό.

```
┌──(root💀 kali)-[~]
└─# nmap -sT - p 443 --script ssl-enum-ciphers 192.168.2.23
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 13:02 EDT
Failed to resolve "-".
Failed to resolve "p".
Stats: 0:00:16 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 50.00% done; ETC: 13:02 (0:00:01 remaining)
Nmap scan report for owaspbwa (192.168.2.23)
Host is up (0.0011s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - D
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
|     compressors:
|       DEFLATE
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - D
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
|     compressors:
|       DEFLATE
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|_  least strength: D
445/tcp   open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:12:37:3A (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (1 host up) scanned in 47.02 seconds
```

Εικόνα 42 Προσδιορισμός κρυπτογράφησης HTTPS

Το SSLScan είναι ένα εργαλείο γραμμής εντολών όσον αφορά στην αξιολόγηση του SSL / TLS διαμόρφωσης διακομιστών. Για να το χρησιμοποιήσουμε, πρέπει να προσθέσουμε μόνο τη διεύθυνση IP του διακομιστή ή όνομα κεντρικού υπολογιστή sslscan 192.168.2.23

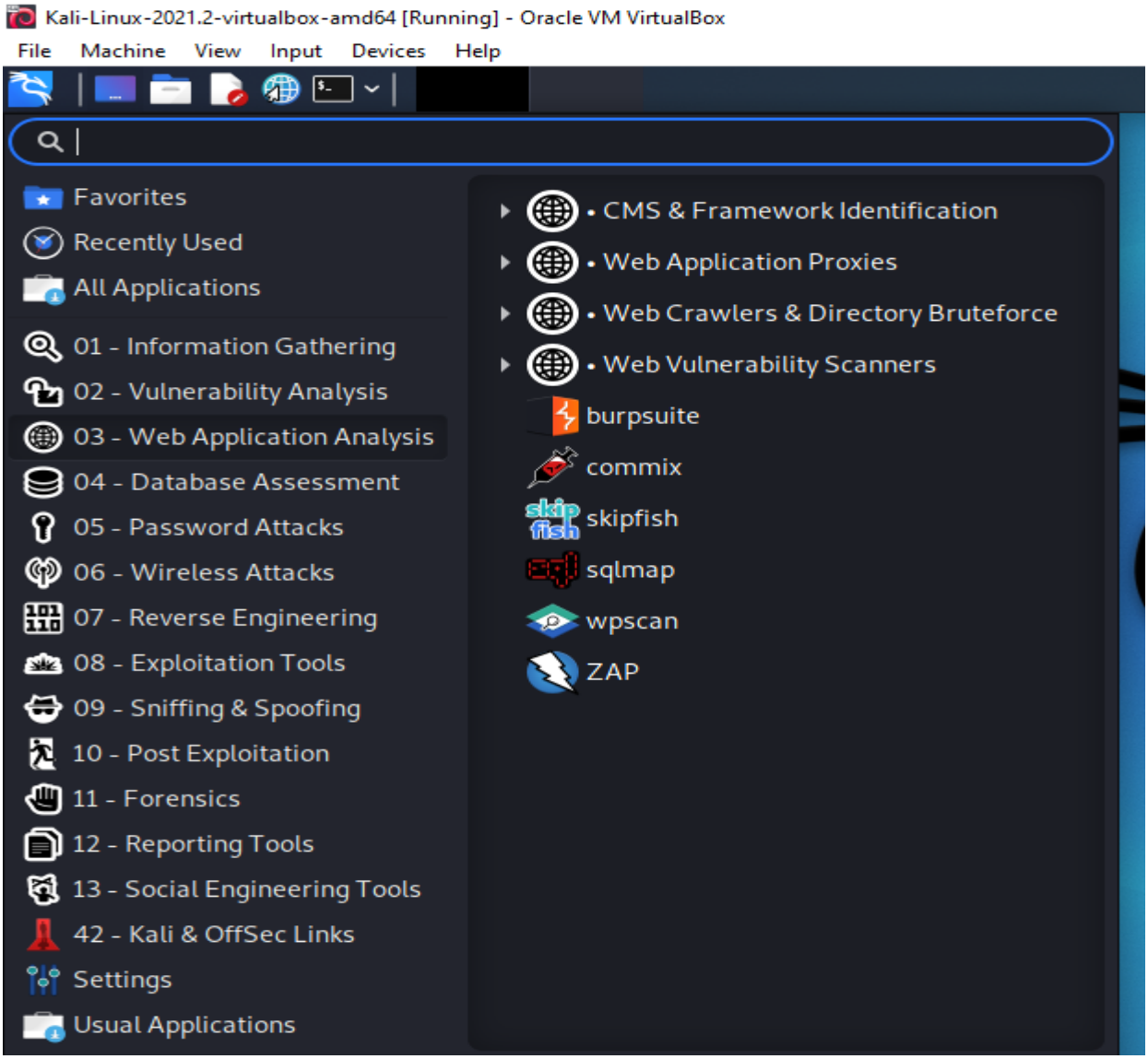
```
┌──(root💀 kali)-[~]
└─# sslscan 192.168.2.23
Version: 2.0.10-static
OpenSSL 1.1.1l-dev  xx XXX xxxx

Connected to 192.168.2.23

Testing SSL server 192.168.2.23 on port 443 using SNI name 192.168.2.23

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     enabled
TLSv1.0   enabled
TLSv1.1   disabled
TLSv1.2   disabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression enabled (CRIME)

  Heartbleed:
TLSv1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.0  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  TLSv1.0  112 bits  DHE-RSA-DES-CBC3-SHA          DHE 1024 bits
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  128 bits  RC4-SHA
Accepted  TLSv1.0  128 bits  RC4-MD5
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA

  SSL Certificate:
Signature Algorithm: sha1WithRSAEncryption
RSA Key Strength:    1024

Subject:  owaspbwa
Issuer:   owaspbwa

Not valid before: Jan  2 21:12:38 2013 GMT
Not valid after:  Dec 31 21:12:38 2022 GMT
```

Εικόνα 43 Εντολή SSLScan για αξιολόγηση SSL/TLS

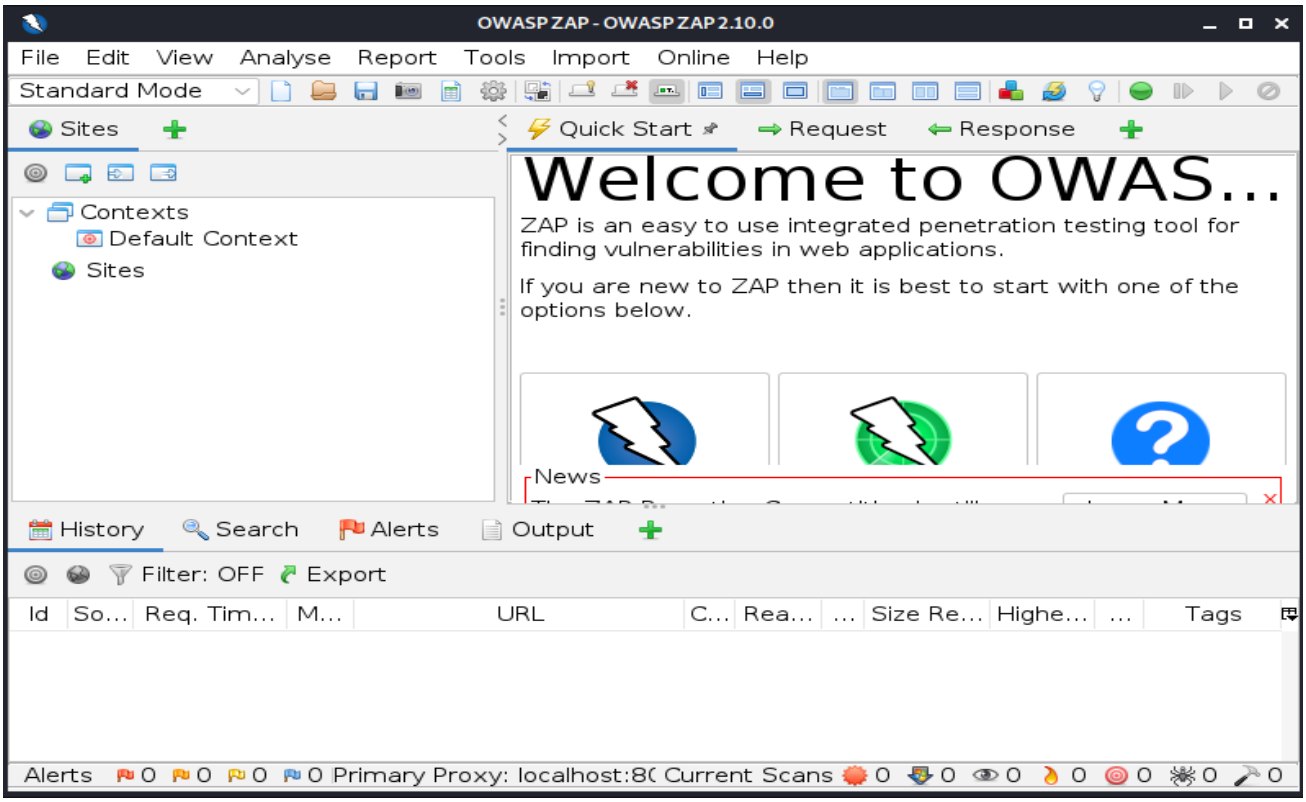
9.7 OWASP ZAP Finding Files and Folders

Το OWASP Zed Attack Proxy (ZAP) είναι ένα πολύ ευέλικτο εργαλείο για τη δοκιμή ασφάλειας ιστού. Έχει έναν διακομιστή μεσολάβησης, παθητικούς και ενεργούς σαρωτές ευπάθειας, fuzzer, spider, αίτημα HTTP αποστολέα και κάποιες άλλες ενδιαφέρουσες δυνατότητες. Θα χρησιμοποιήσουμε το Forced Browse, το οποίο είναι η υλοποίηση του DirBuster μέσα στο ZAP. Πρέπει να χρησιμοποιήσουμε το ZAP ως διακομιστή μεσολάβησης για το πρόγραμμα περιήγησης ιστού. Για να ξεκινήσουμε το OWASP ZAP από το main menu του Kali Linux επιλέγουμε το 03 Web Application Analysis όπως φαίνεται στην εικόνα 44 . Πρέπει να ρυθμίσουμε τον διακομιστή μεσολάβησης στο ZAP. από αυτή της θύρας προεπιλογής.8080 σε 8090.

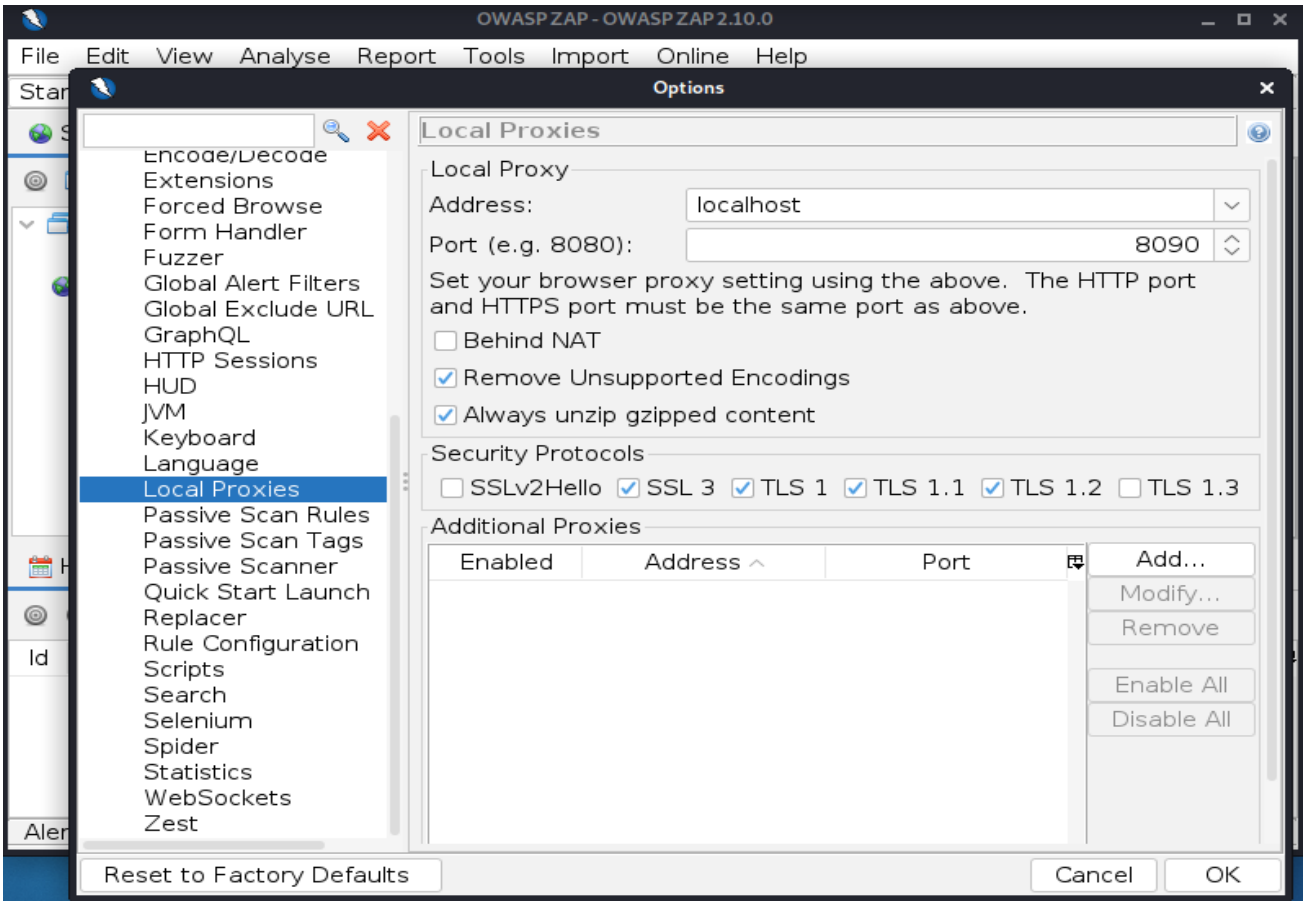
Στο main menu - Tools-Option-Local proxies στο πεδίο Address πληκτρολογούμε localhost στο πεδίο port βάζουμε 8090 όπως φαίνεται στην εικόνα 46.



Εικόνα 44 Πρόγραμμα ZAP στο λειτουργικό Kali Linux

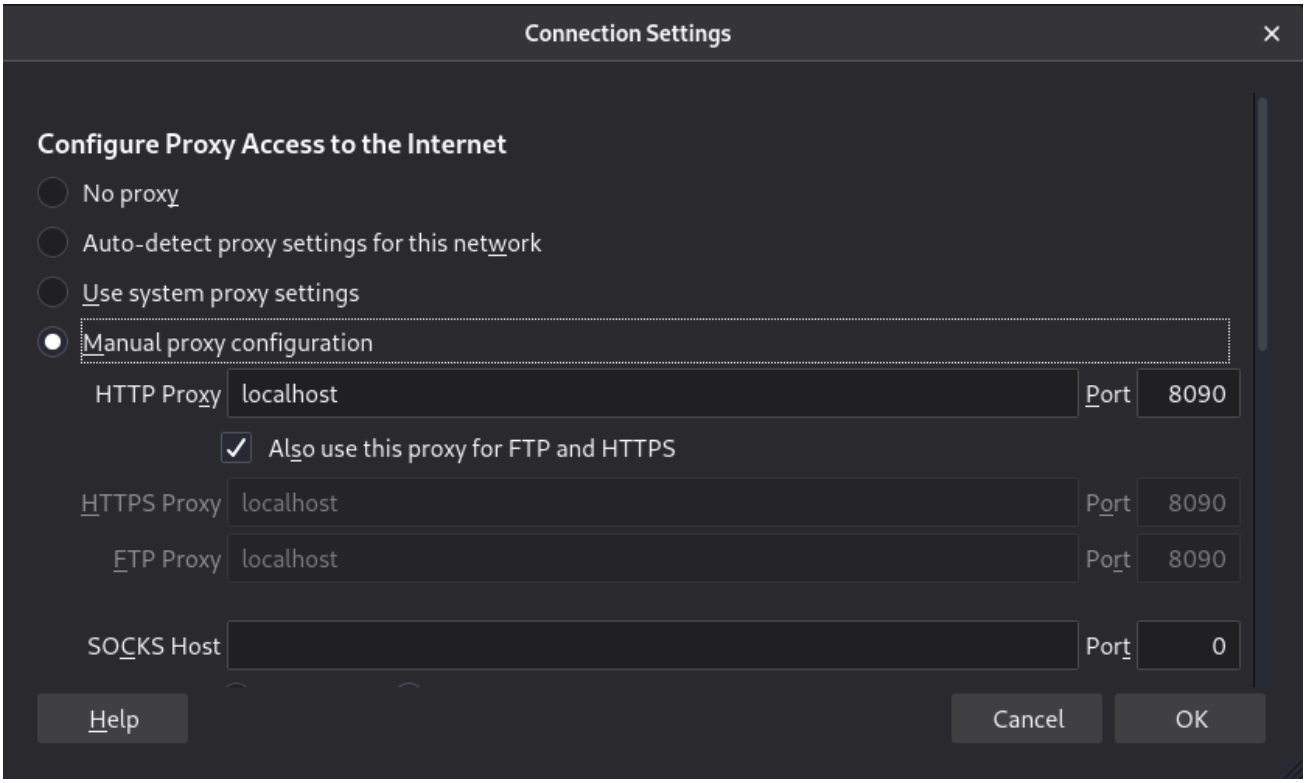


Εικόνα 45 Γραφικό περιβάλλον εφαρμογής ZAP



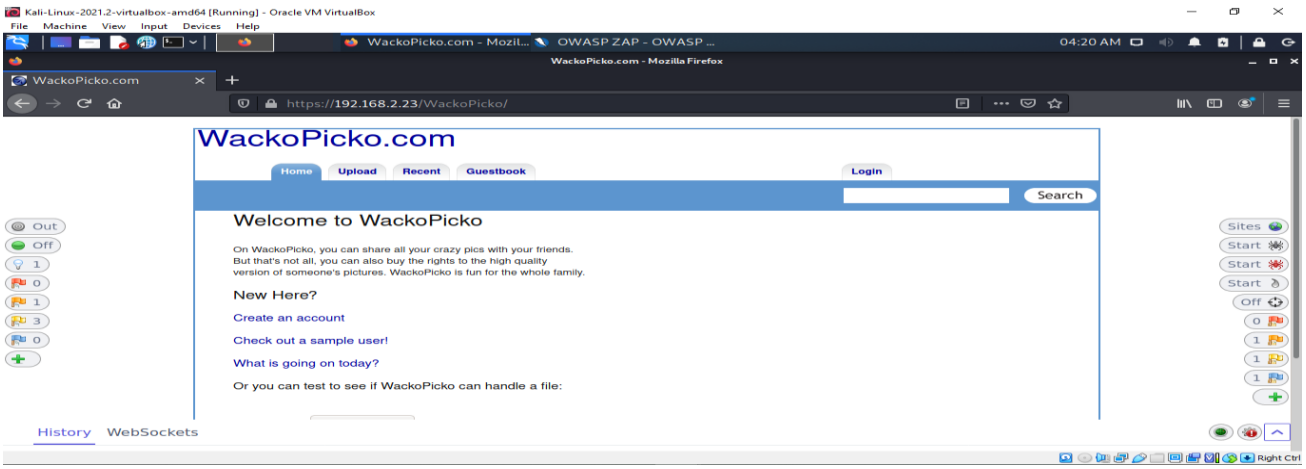
Εικόνα 46 Ρύθμιση Local Proxies στην εφαρμογή ZAP

Στον Firefox του Kali Linux, στο κύριο μενού, στις προτιμήσεις, στις ρυθμίσεις δικτύου επιλέγουμε ρυθμίσεις και βάζουμε χειροκίνητο proxy localhost και την πόρτα 8090 όπως τα βάλαμε και στο zap όπως φαίνεται στην εικόνα 47.

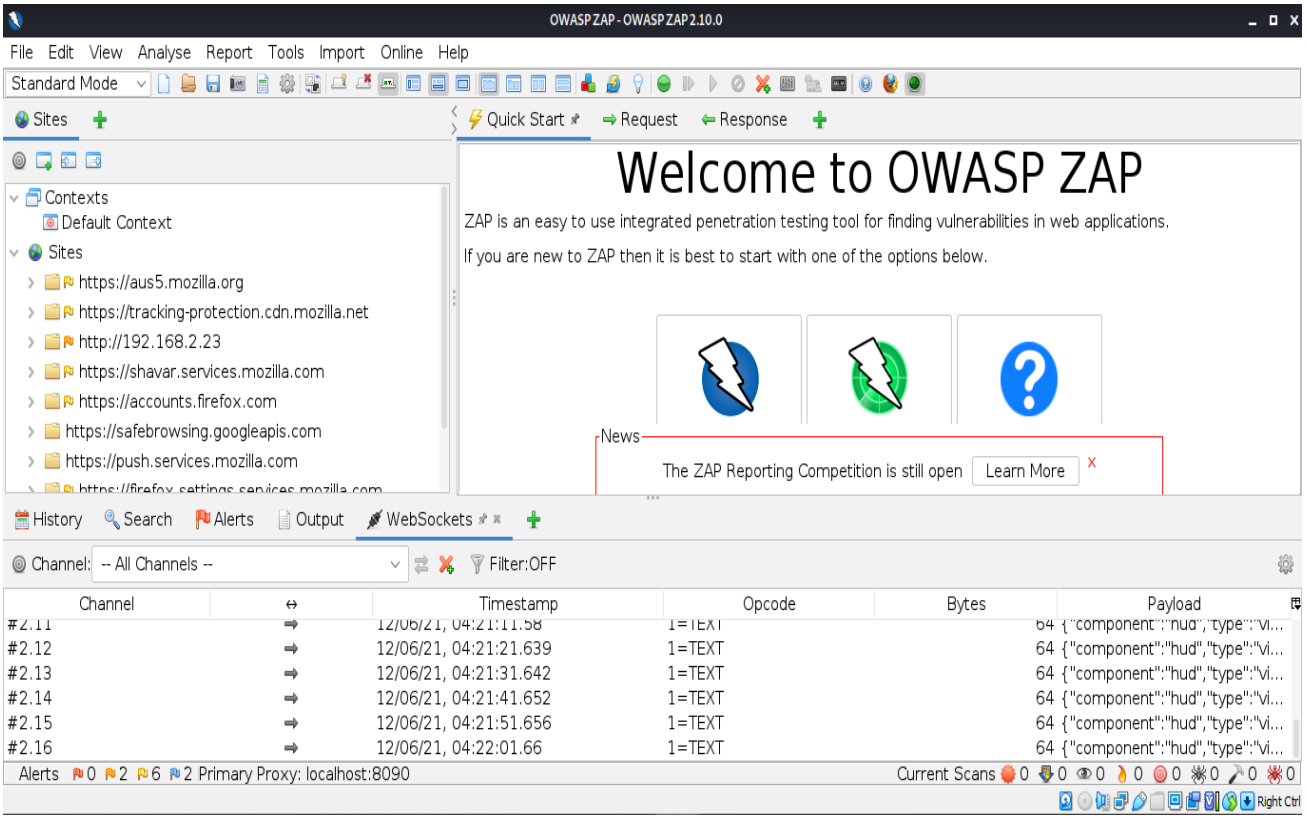


Εικόνα 47 Ρυθμίσεις Mozilla Firefox στο Kali Linux

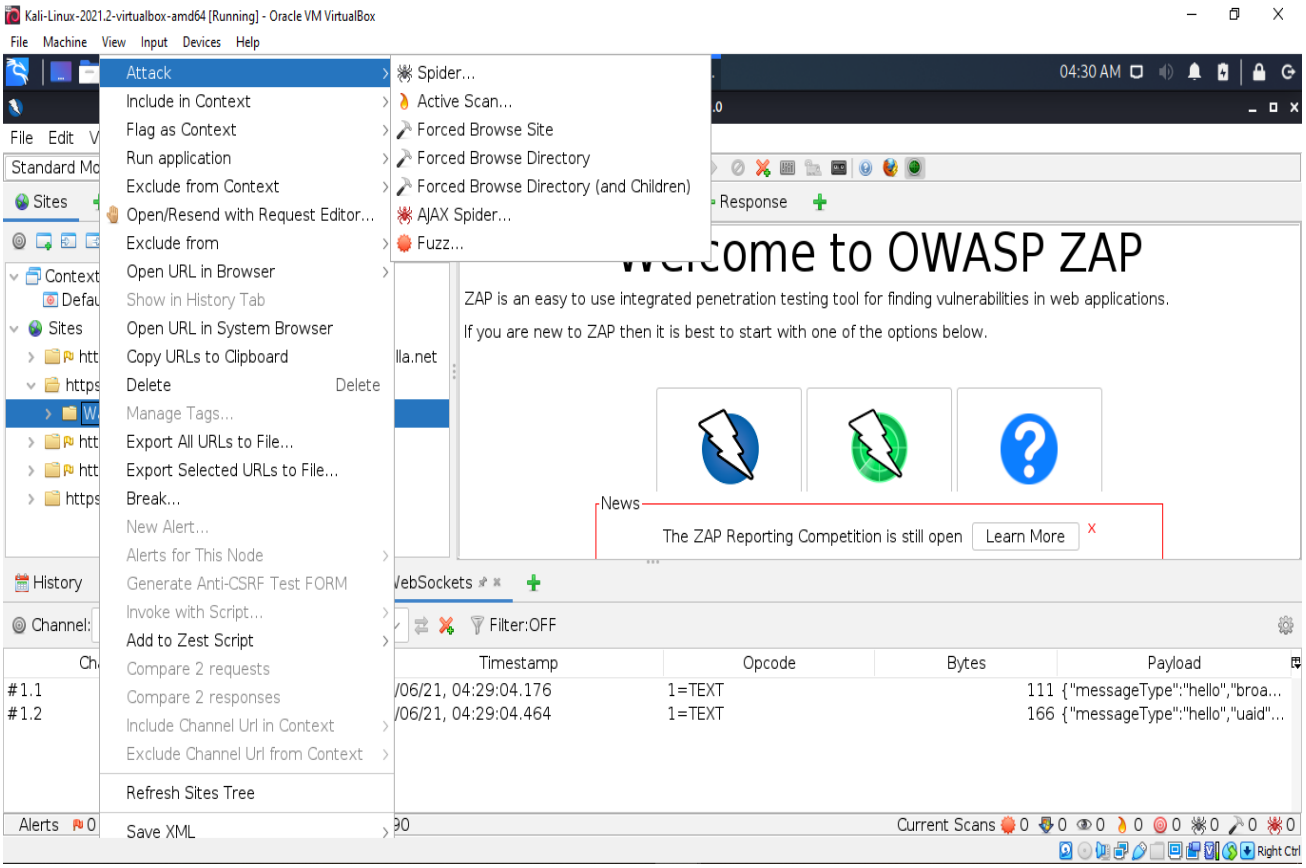
Αφού έχουμε ρυθμίσει τον browser και τον Proxy είμαστε έτοιμοι να αναζητήσουμε τον Server για φάκελους που υπάρχουν. Αναζητούμε από τον browser http://192.168.56.11/WackoPicko . Στο ZAP βλέπουμε ότι αντιδρά και φέρνει την δομή δέντρου του Host που επισκεφτήκαμε. Στον επάνω αριστερό πίνακα του ZAP, στην καρτέλα Ιστότοπου κάνουμε δεξί κλικ στο φάκελο WackoPicko. Στη συνέχεια, στο μενού περιβάλλοντος στο Attack και Forced Browse directory (and children). αυτό θα κάνει μια σάρωση. όπως φαίνεται στις εικόνες 49-52.



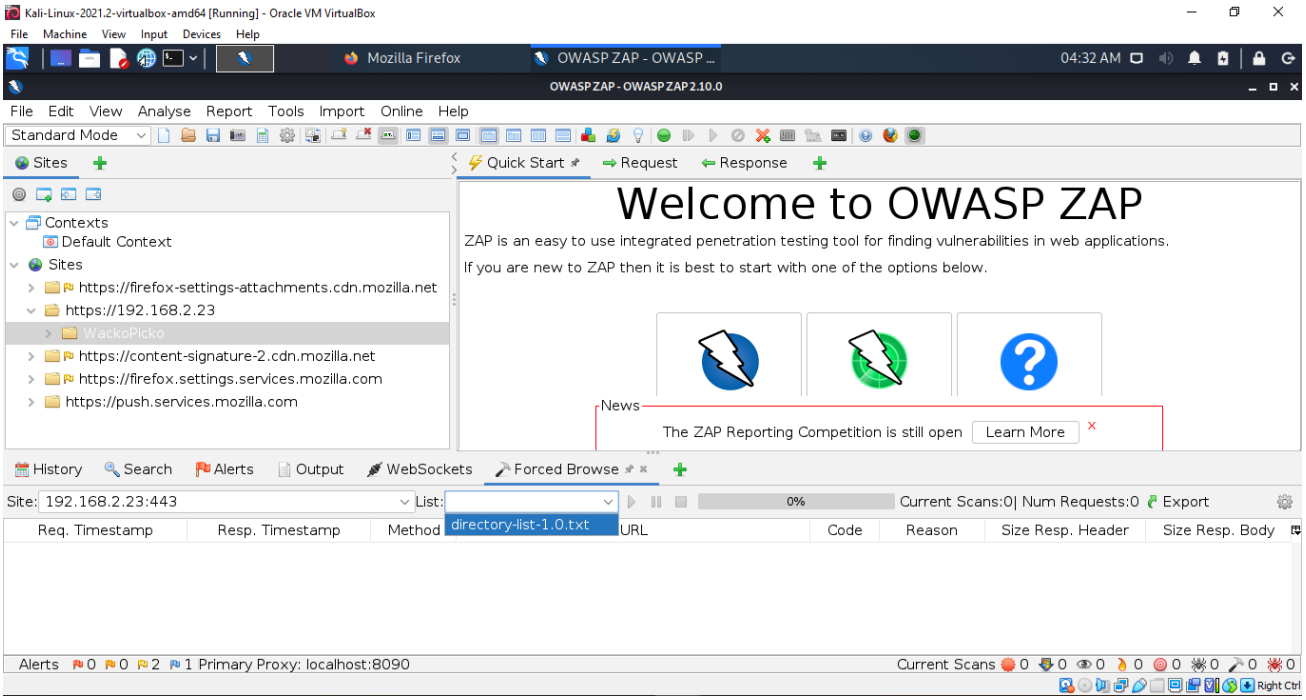
Εικόνα 48 Αναζητούμε από τον browser http://192.168.56.11/WackoPicko



Εικόνα 49 Στο ZAP βλέπουμε ότι φέρνει την δομή Host που επισκεφτήκαμε

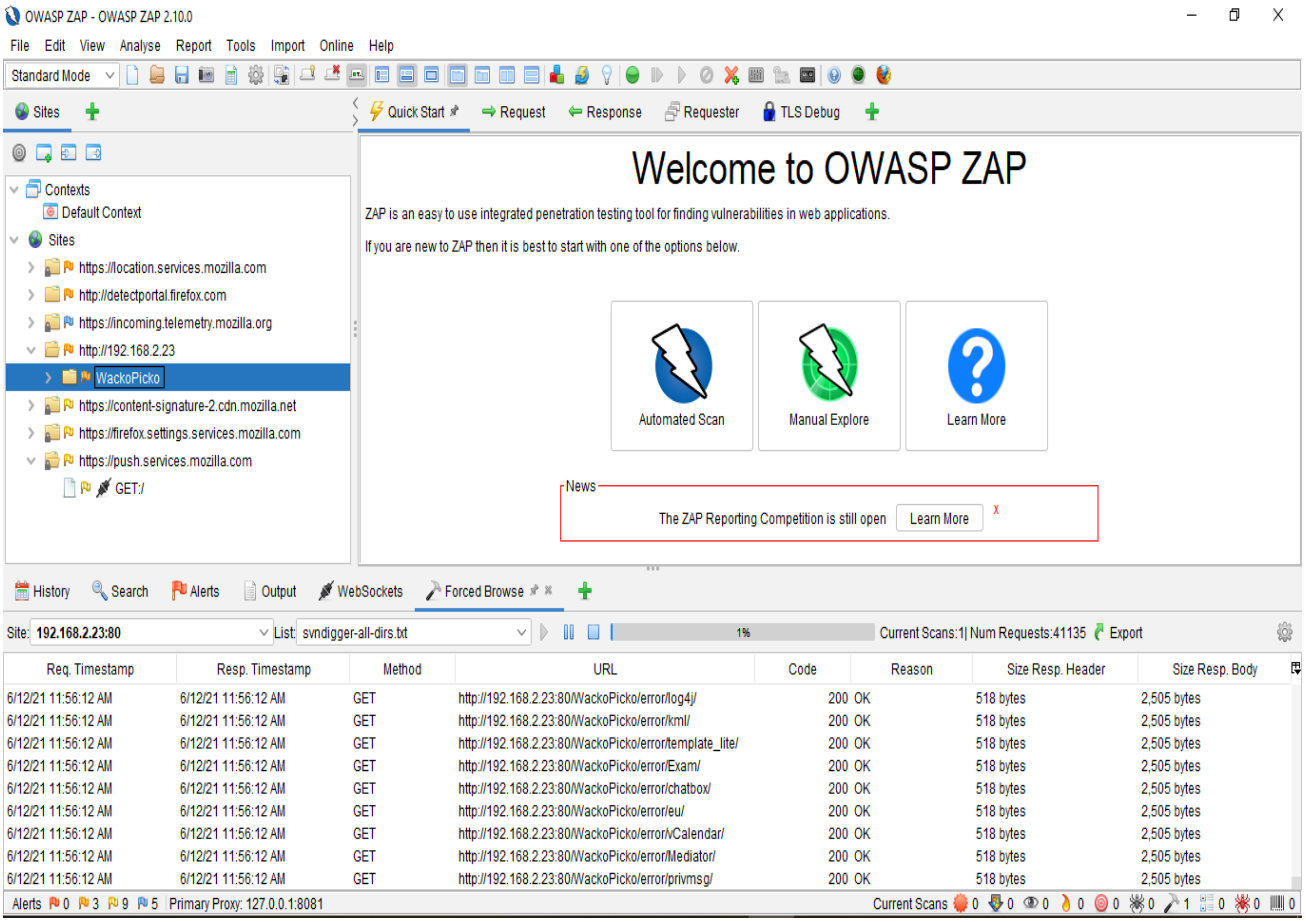


Εικόνα 50 Attack και Forced Browse directory (and children)



Εικόνα 51 Έναρξη σάρωσης

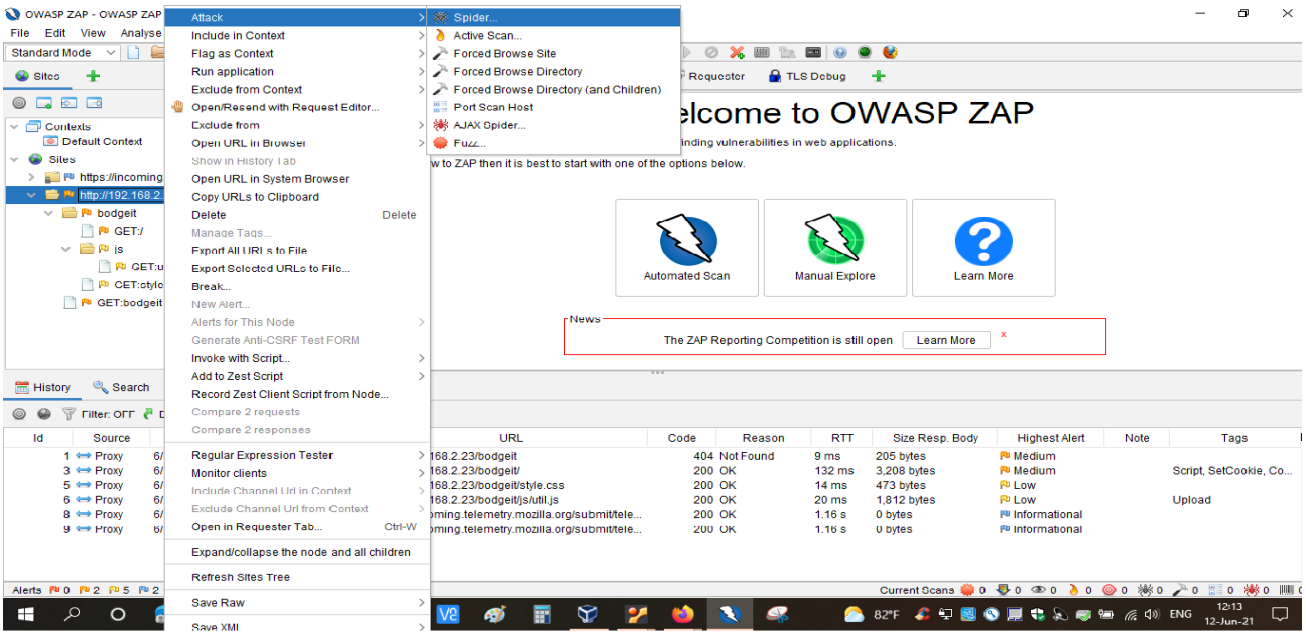
Στον εικόνα 51εμφανίζεται η καρτέλα Forced Browse και βλέπουμε την πρόοδο της σάρωσης και τα αποτελέσματά της στην εικόνα 52.



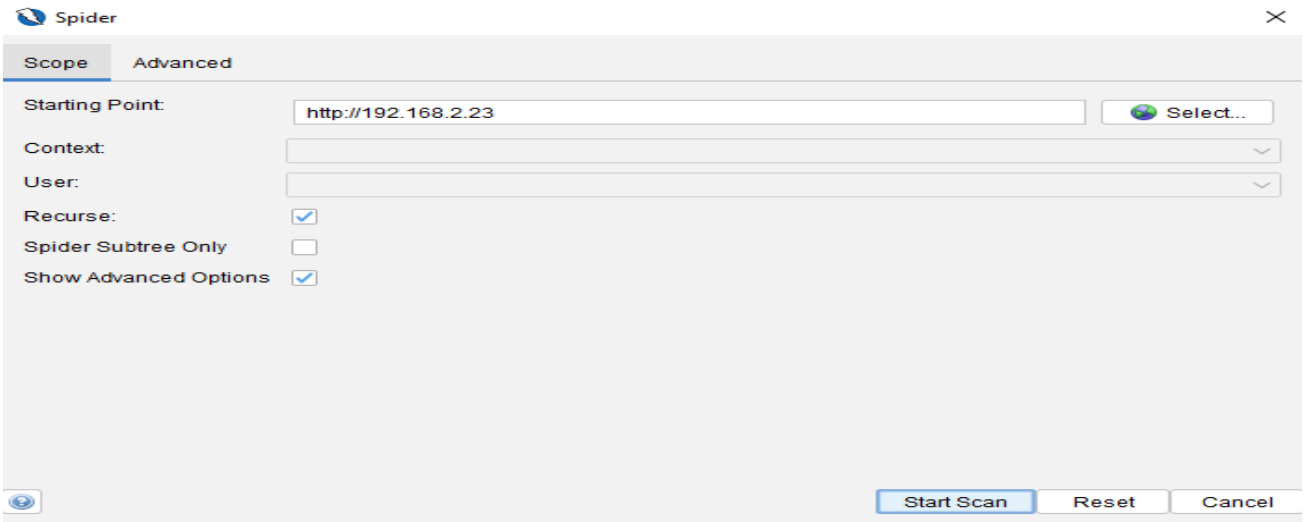
Εικόνα 52 Πρόοδος σάρωσης Forced Browse

9.8 OWASP ZAP Spider

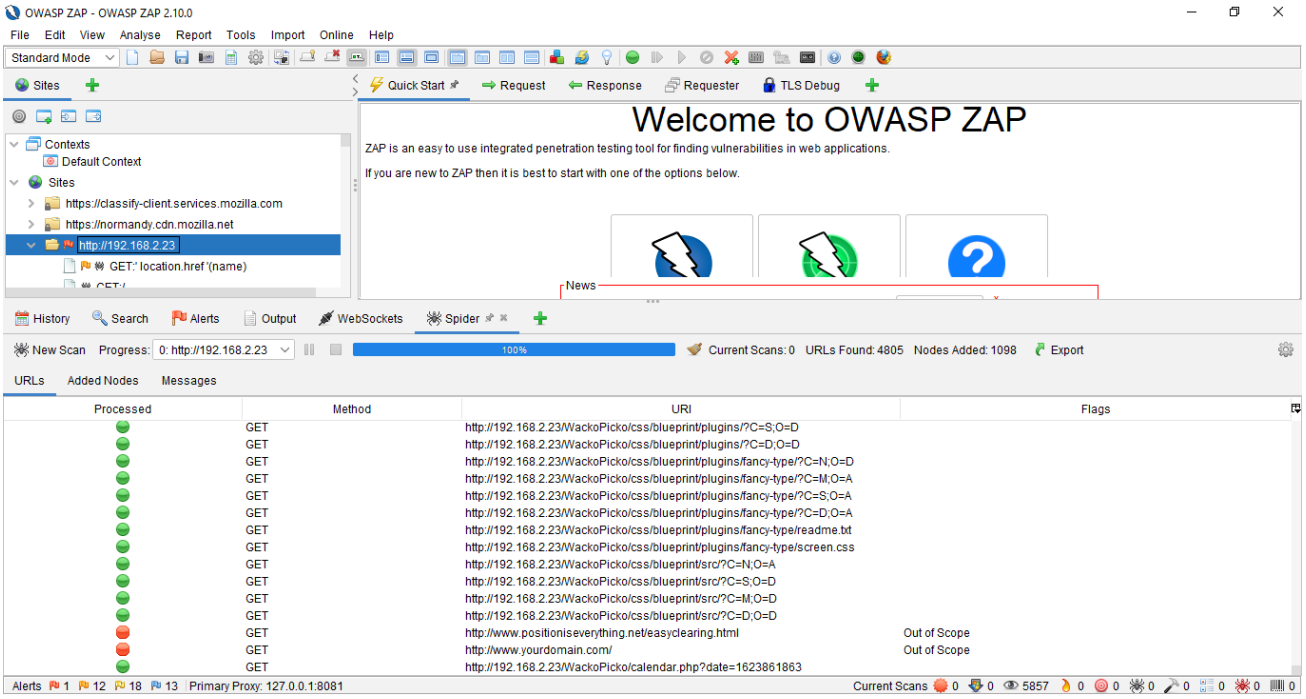
Στις εφαρμογές ιστού, ένα πρόγραμμα ανίχνευσης ή αράχνη είναι ένα εργαλείο που περνά αυτόματα από ένα ιστότοπο που ακολουθεί όλους τους συνδέσμους σε αυτόν και μερικές φορές συμπληρώνει και στέλνει φόρμες. Αυτό επιτρέπει να λάβουμε έναν πλήρη χάρτη όλων των σελίδων που αναφέρονται στον ιστότοπο και να καταγράψουμε τα αιτήματα που υποβλήθηκαν για να λάβουμε αυτές και τις απαντήσεις τους.
Θα χρησιμοποιήσουμε το BodgeIt (http://192.168.56.11/bodgeit/) για να δείξουμε πώς λειτουργεί η αράχνη του ZAP. Στην καρτέλα ιστότοποι, ανοίξτε το φάκελο που αντιστοιχεί στην τοποθεσία δοκιμής http://192.168.2.23, κάνουμε δεξί κλικ στο GET: bodgeit και από το αναπτυσσόμενο μενού επιλέξτε Attack και Αράχνη όπως φαίνεται στην εικόνα 53.



Εικόνα 53 Attack Spider στο http://192.168.56.11/bodgeit/

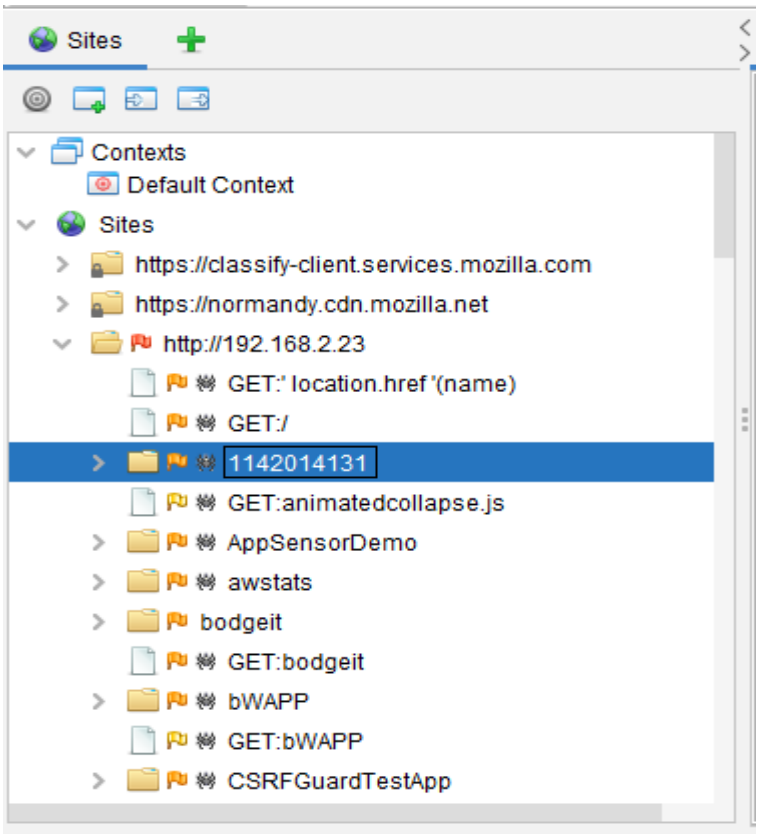


Εικόνα 54 Πατάμε start scan με τα default settings



Εικόνα 55 Αποτελέσματα στο Spider tab μετά το scan

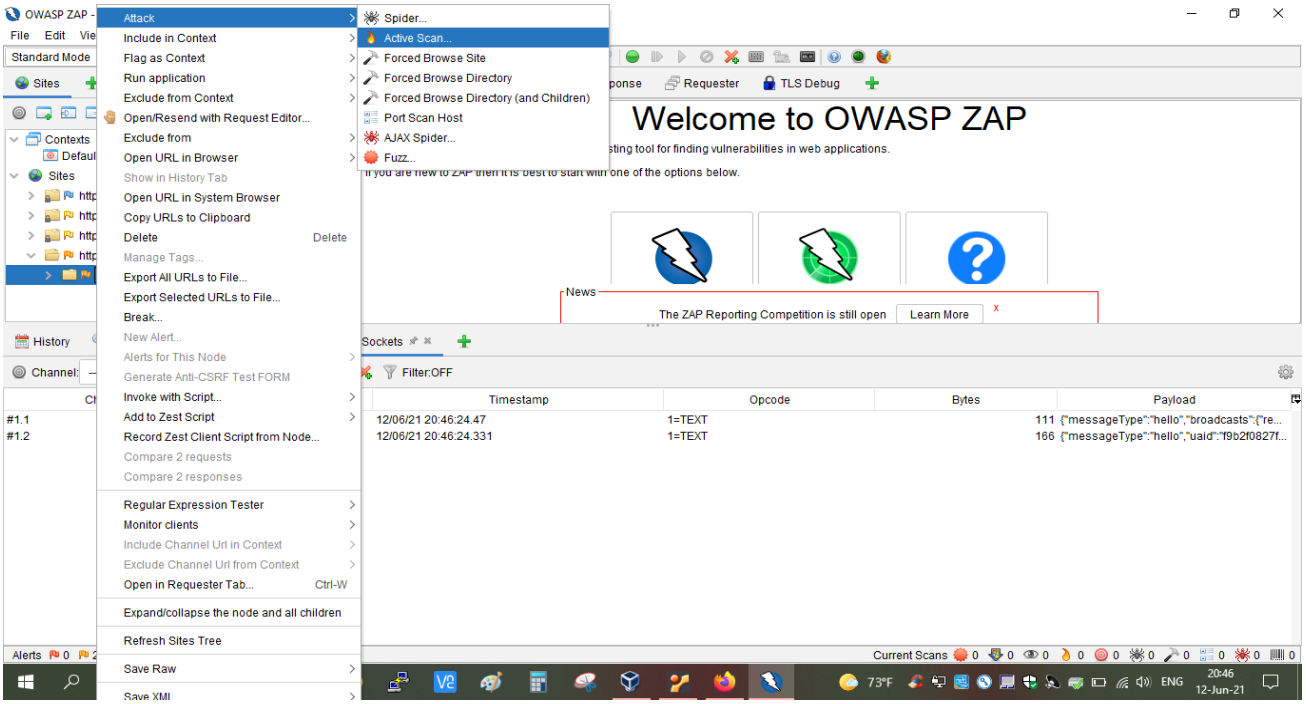
Εάν θέλουμε να αναλύσουμε τα αιτήματα και τις απαντήσεις μεμονωμένων αρχείων, πηγαίνουμε στο καρτέλα ιστότοποι και ανοίγουμε τον φάκελο του ιστότοπου και κοιτάμε τα αρχεία και τους φακέλους μέσα σε αυτόν όπως φαίνεται στην εικόνα 56.



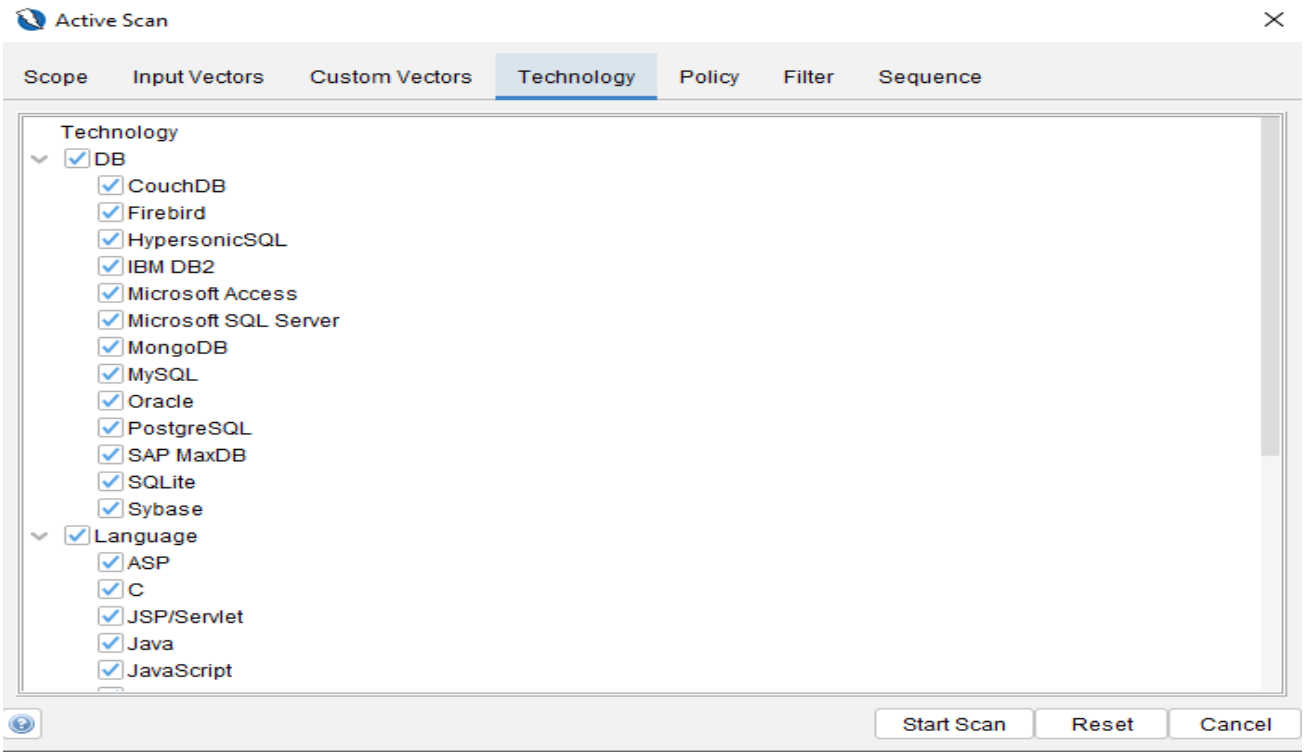
Εικόνα 56 Αρχεία και φάκελοι ιστότοπου

9.9 OWASP ZAP Scan Vulnerabilities

Το OWASP ZAP είναι ένα εργαλείο που περιλαμβάνει έναν αυτόματο σαρωτή ευπάθειας. Επισκεπτόμαστε την σελίδα http://192.168.56.11/peruggia/ και ξεκινάμε το πρόγραμμα ανίχνευσης Active Scan όπως φαίνεται στην εικόνα 57.



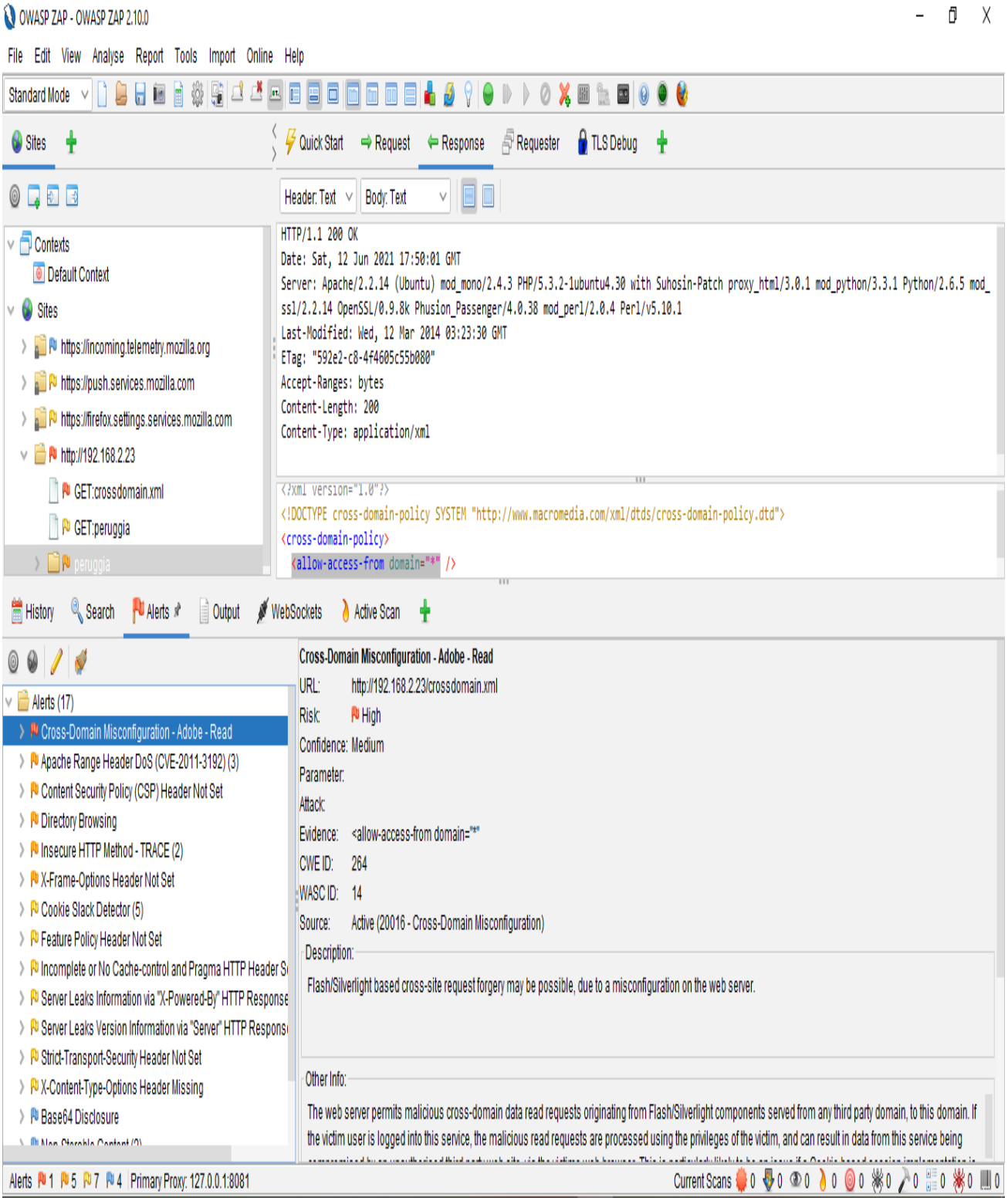
Εικόνα 57 Πρόγραμμα ανίχνευσης spider στο φάκελο peruggia



Εικόνα 58 Τεχνολογίες εφαρμογής και Server

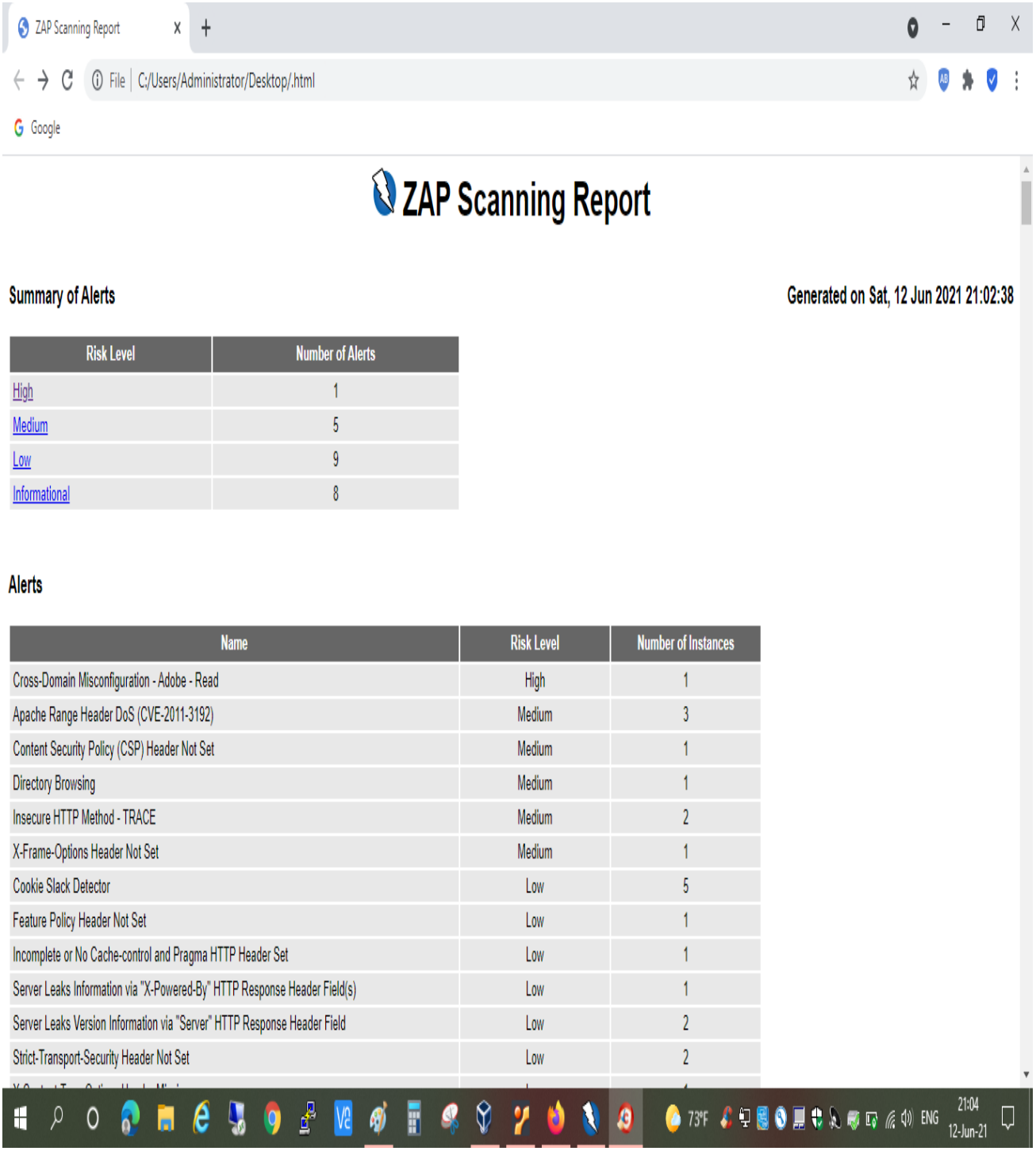
Επιλέγουμε μόνο MySQL,PHP, Linux, και Apache και πατάμε Start Scan όπως φαίνεται στην εικόνα 58.

Εάν επιλέξουμε μια ειδοποίηση, μπορούμε να δούμε το αίτημα που υποβλήθηκε και την απόκριση που ελήφθη από τον διακομιστή. Αυτό μας επιτρέπει να αναλύσουμε την επίθεση και να προσδιορίσουμε αν είναι αληθινή ευπάθεια.



Εικόνα 59 Vulnerabilities Alerts

Για την εξαγωγή ενός HTML report, επιλέγουμε Reports από το main menu και μετά Generate HTML Report και κάνουμε save στο path που επιθυμούμε.



Εικόνα 60 Zap Scanning Report

10 Σύνοψη

Τα ενσωματωμένα συστήματα και το Διαδίκτυο των πραγμάτων αποτελούν ραγδαία εξελισσόμενες μορφές τεχνολογίας με μεγάλο εύρος εφαρμογής σε όλους τους τομείς. Μετά την ανεξέλεγκτη αύξηση της παραγωγής συσκευών IOT από εταιρίες χωρίς κεντρικό σχεδιασμό για τα επίπεδα ασφάλειας της συσκευής, κατέστη αναγκαία η παρακολούθηση και η σωστή διαχείριση των συσκευών για την αύξηση των επιπέδων ασφαλείας σε ολόκληρη την αλυσίδα ανεφοδιασμού. Από την αρχή της εφαρμογής αυτών των τεχνολογιών παρατηρούνται πολλαπλές μορφές επιθέσεων στον Κυβερνοχώρο, οι οποίες οδήγησαν στον σχεδιασμό και την ανάπτυξη διεθνών και ευρωπαϊκών προδιαγραφών ώστε να διασφαλιστεί η ποιότητα των συστημάτων. Στην παρούσα εργασία παρουσιάστηκαν οι καλές πρακτικές, οι διαδικασίες και οι τεχνολογίες που έχουν εξελιχθεί για την ασφάλεια της αλυσίδας IOT. Στις δοκιμές διείσδυσης παρουσιάστηκαν μέσω του ανοιχτού λογισμικού Kali Linux οι τρόποι συλλογής πληροφοριών για την κατάσταση διακομιστή και τι είδους υπηρεσίες ή λειτουργικό σύστημα εκτελείται και σε ποιες θύρες. Επίσης έγινε έλεγχος για την ύπαρξη τείχους προστασίας σε όλες τις HTTP Θύρες και προσδιορισμός και αξιολόγηση κρυπτογράφησης. Με το OWASP ZAP έγινε εύρεση φακέλων και αρχείων του διακομιστή και σάρωση για εύρεση και αξιολόγηση πιθανών ευπαθειών. Οι δοκιμές διείσδυσης οδηγούν σε εύρεση των κενών ασφαλείας με απώτερο σκοπό την θωράκιση των συστημάτων από κακόβουλους εισβολείς.

11 Βιβλιογραφία – Πηγές

[1] "Embedded system", En.wikipedia.org, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Embedded_system. Accessed: 15- Feb- 2021]

[2] S. Heath, Embedded systems design, 2nd ed. Oxford: Newnes, 2003, pp. 1-2.

[3] M. Barr and A. Massa. Programming Embedded Systems. O'Reilly, 2nd edition, 2006, pp 2

[4] F. Xiacong, Real-Time Embedded Systems Design Principles and Engineering Practices. Oxford: Newnes, 2015, p. 14.

[5] J. Wang, Real-Time Embedded Systems. Hoboken: Willey, 2017, p. 1-3.

[6] Μ. Δασυγένης και Δ. Σούντρης, Ενσωματωμένα Συστήματα Ο αθέατος ψηφιακός κόσμος: Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα,2015, p 35-36

[7] M. Swan, "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0", Journal of Sensor and Actuator Networks, vol. 1, no. 3, pp. 217-253, 2012. Available: 10.3390/jsan1030217.

[8] "IoT technology stack - IoT devices, sensors, gateways and platforms", i-SCOOP, 2021. [Online]. Available: https://www.i-scoop.eu/internet-of-things-guide/iot-technology-stack-devices-gateways-platforms/. [Accessed: 15- Feb- 2021].

[9] Smart Life Saver System forAlzheimer Patients, down Syndromes, and Child Missing Using IoT - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/IoT-Sensors-and-Actuators_fig4_324877806 [accessed 15 Feb, 2021]

[10] K. Rose, S. Eldridge and L. Chapin, The Internet Of Things: An Overview Understanding the Issues and Challenges of a More Connected World. The Internet Society (ISOC), 2015, pp. 9, 18-22.

[11] An Overview of Security Issues Relating to the Internet of Things - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Example-of-device-to-device-communication-model_fig1_334603508 [accessed 15 Feb, 2021]

[12] An Overview of Security Issues Relating to the Internet of Things - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Device-to-cloud-communication-model-diagram_fig2_334603508 [accessed 15 Feb, 2021]

[13] An Overview of Security Issues Relating to the Internet of Things - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Device-to-gateway-communication-model-diagram_fig3_334603508 [accessed 15 Feb, 2021]

[14] A Review On Internet Of Things Architecture For Big Data Processing - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Back-End-Data-Sharing-Model_fig4_343514386 [accessed 15 Feb, 2021]

[15] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues", Computer Networks, vol. 144, pp. 17-39, 2018. Available: 10.1016/j.comnet.2018.07.017 [Accessed 2 February 2021].

[16] Enisa.europa.eu, 2021. [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures. [Accessed: 06- Jan- 2021].

[17] "What is IoT? Tips for IoT Security", www.kaspersky.com, 2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-iot. [Accessed: 18- Dec- 2020].

[18] "Internet of Things Global Standards Initiative", Itu.int, 2021. [Online]. Available: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx. [Accessed: 04- Jan- 2021].

[19] "What is an IoT Gateway? Open Automation Software",*Open Automation Software*, 2021. [Online]. Available: https://openautomationsoftware.com/open-automation-systems-blog/what-is-an-iot-gateway/. [Accessed: 04- Feb- 2021].

[20] I. Smith, The Internet of Things 2012 New Horizons, 3rd ed. Halifax, UK: IERC, 2012, pp. 35-39.

[21] M. Staff, "Top 10 Emerging IoT Technologies You Need to Know", Material Handling and Logistics, 2021. [Online]. Available: https://www.mhlnews.com/technology-automation/article/22051554/top-10-emerging-iot-technologies-you-need-to-know. [Accessed: 18- Dec- 2020].

[22] "What technologies are used in IoT – technology behind Internet of Things", *Avsystem.com*, 2021. [Online]. Available: https://www.avsystem.com/blog/iot-technology/. [Accessed: 03- Jan- 2021].

[23] *ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025*. Athens: ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ, 2020, pp. 9-14.

[24] "What is a Cyber Threat? | UpGuard", *Upguard.com*, 2021. [Online]. Available: https://www.upguard.com/blog/cyber-threat [Accessed: 06- Mar- 2021].

[25] M. Lourenço and L. Marinos, *ENISA Threat Landscape - The year in review*. © European Union Agency for Cybersecurity (ENISA), 2020, 2019, p. 7.

[26] C. Skouloudi, A. Malatras and R. Naydenov, *GUIDELINES FOR SECURING THE INTERNET OF THINGS*. European Union Agency for Cybersecurity (Enisa), 2020, 2020, pp. 9-36.