ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Μελέτη Συστημάτων και Τεχνικών Επιβλεπόμενης Μάθησης για την Ανίχνευση Εισβολών με βάση δημοσίως διαθέσιμα Σύνολα Δεδομένων στο πεδίο αυτό

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ηλίας Αντωνιάδης

Επιβλέπουσα καθηγήτρια: Θεοδώρα Βαρβαρίγου, Καθηγήτρια Ε.Μ.Π.

Αθήνα, Ιούνιος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Μελέτη Συστημάτων και Τεχνικών Επιβλεπόμενης Μάθησης για την Ανίχνευση Εισβολών με βάση δημοσίως διαθέσιμα Σύνολα Δεδομένων στο πεδίο αυτό

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ηλίας Αντωνιάδης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις 6 Ιουνίου 2022.

……..…….……	……..…….……	……..…….……
Θεοδώρα Α. Βαρβαρίγου	Δημήτριος Ασκούνης	Ιωάννης Ψαρράς
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2022

……

Ηλίας Αντωνιάδης

Ηλεκτρολόγος Μηχανικός & Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών.

ΠΕΡΙΛΗΨΗ

Τα συστήματα ανίχνευσης εισβολών αποτελούν τη σημαντικότερη γραμμή άμυνας απέναντι στις επιθέσεις δικτύων. Εξαιτίας της έλλειψης αξιόπιστων συστημάτων επαλήθευσης και επικύρωσης, έχει αναπτυχθεί μία ποικιλία τεχνικών καθώς και συνδυασμός αυτών, με σκοπό την ανίχνευση εισβολών, είτε σε επίπεδο host είτε σε επίπεδο network.

Σκοπός της παρούσας διπλωματικής εργασίας αποτελεί, μία αρχική αναζήτηση, μελέτη και παρουσίαση των ήδη υπαρχόντων συστημάτων ανίχνευσης εισβολών, έπειτα η χρήση επιλεγμένου συνόλου δεδομένων από κυβερνοεπιθέσεις και η εφαρμογή αλγορίθμων ταξινόμησης για την ανίχνευση εισβολών, και τέλος η αξιολόγηση αποτελεσμάτων συνοδευόμενα από τα αντίστοιχα συμπεράσματα που προέκυψαν.

ΛΕΞΕΙΣ - ΚΛΕΙΔΙΑ

Τεχνικές επιβλεπόμενης μάθησης, ταξινόμηση, ανίχνευση εισβολών.

ABSTRACT

Intrusion Detection Systems (IDSs) are the most important defense line against network attacks. Nowadays, due to the lack of reliable verification and validation systems, a variety of techniques has been developed as well as a combination of them, in order to detect intrusions, either at host or network level.

The purpose of this thesis is, thus, an initial search, study and presentation of the already existing intrusion detection systems, then the use of a selected cybersecurity dataset as well as the implementation of classification algorithms for intrusion detection, and finally the results evaluation accompanied by the corresponding conclusions emerged.

KEYWORDS

Supervised learning techniques, classification, intrusion detection.

ΕΥΧΑΡΙΣΤΙΕΣ

Οφείλω να ευχαριστήσω την Καθηγήτρια του Ε.Μ.Π. Κα Θεοδώρα Βαρβαρίγου, για την ευκαιρία που είχα να ασχοληθώ στη διπλωματική μου εργασία με τον τομέα την μηχανικής μάθησης. Εκτιμώ την συνεχή βοήθεια, επαρκή καθοδήγηση και πλήρη συνεισφορά του Διδάκτορα Ευθύμιου Κ. Χονδρογιάννη, ο οποίος με ενέπνευσε ενεργά στην εκπόνηση της συγγραφής αυτής, μεταφέροντας πέρα από την τεχνική γνώση, και το ότι η μηχανική μάθηση είναι, κατά κάποιο τρόπο, περισσότερο τέχνη παρά επιστήμη. Ευχαριστώ, με την ευκαιρία, τους κοντινούς μου ανθρώπους, που μου δίδαξαν άμεσα ή έμμεσα, την ετυμολογία της κριτικής σκέψης, συνεισφέροντας έτσι στην ικανότητα τοποθέτησης των βασικών αρχών και απώτερων στόχων της 4ης βιομηχανικής επανάστασης σε ένα ισοζύγιο. Ευελπιστώντας εν τέλει στην εφαρμογή της αυτοματοποιημένης τεχνολογικής ανταλλαγής δεδομένων διά του "ὠφελέειν ἢ μὴ βλάπτειν".

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1: Εισαγωγή

Υπάρχουν συστήματα ανίχνευσης εισβολών (intrusion detection systems, IDS), τα οποία βασίζονται σε αλγορίθμους μηχανικής μάθησης. Τα συστήματα αυτά χωρίζονται σε "signature based" και "anomaly based" τεχνικές ανίχνευσης απειλών. Τα signature based χρησιμοποιούνται για να ανιχνεύσουν γνωστές απειλές. Λειτουργούν χρησιμοποιώντας δηλαδή τις ήδη προγραμματισμένες λίστες απειλών και τους δείκτες συμβιβασμού (indicators of compromise, IOCs) αυτών. Ένας τέτοιος δείκτης μπορεί να είναι μία συγκεκριμένη συμπεριφορά που προηγείται μίας κακόβουλης επίθεσης δικτύου, μείγματα αρχείων (file hashes), κακόβουλοι χώροι δικτύου (malicious domains), γνωστές ακολουθίες από bytes (bytes sequences), ή ακόμα και το περιεχόμενο από επικεφαλίδες email μηνυμάτων. Τα signature based συστήματα παρακολουθούν τα πακέτα που μεταφέρονται στο δίκτυο, τα συγκρίνουν με τα γνωστά μηνύματα που υπάρχουν σε βάσεις δεδομένων γνωστών δεικτών συμβιβασμού, ή υπογραφών επιθέσεων, με σκοπό να σημειώσουν ύποπτη κακόβουλη συμπεριφορά. Από την άλλη πλευρά, τα anomaly based συστήματα μπορούν να ειδοποιήσουν για ύποπτη συμπεριφορά η οποία είναι άγνωστη. Δεν εφαρμόζουν δηλαδή αναζήτηση σε γνωστές απειλές, αντιθέτως χρησιμοποιούν αλγορίθμους μηχανικής εκμάθησης με σκοπό να εκπαιδεύσουν το σύστημα ανίχνευσης έτσι ώστε να αναγνωρίζει μία κανονικοποιημένη γραμμή βάσης (normalized baseline). Η γραμμή αυτή αντιστοιχεί στο πώς το σύστημα συμπεριφέρεται σε κανονικές συνθήκες, και έπειτα η δραστηριότητα δικτύου συγκρίνεται με τη γραμμή αυτή.

Στην παρούσα διπλωματική εργασία θα γίνει αρχικά μία επισκόπηση των εργαλείων ανίχνευσης εισβολών καθώς των συνόλων δεδομένων τα οποία είναι δημοσίως διαθέσιμα, και ακολουθεί εφαρμογή μεθοδολογίας και αλγορίθμων μηχανικής μάθησης με σκοπό την ανίχνευση εισβολών με βάση επιλεγμένο σύνολο δεδομένων. Σχετικά με τα συστήματα, έγινε αναζήτηση αυτών που είναι διαθέσιμα και αναλύονται συστήματα host based (host based intrusion detection systems, HIDS), network based (network based intrusion detection systems, NIDS) καθώς και υβριδικά που χρησιμοποιούν HIDS και NIDS. Πρακτικά τα πρώτα αναζητούν host-based συμπεριφορές (σε επίπεδο endpoint) συμπεριλαμβάνοντας τις εφαρμογές που χρησιμοποιήθηκαν, τα αρχεία που προσπελάστηκαν, και την πληροφορία που αποθηκεύτηκε σε αρχεία πυρήνα (kernel log files). Τα δεύτερα, εξετάζουν τις ροές δεδομένων (data flows) μεταξύ υπολογιστών, γνωστές και ως κίνηση δικτύου (network traffic). Σχετικά

με τα σύνολα δεδομένων, αναλύθηκαν δημοσίως διαθέσιμα σύνολα δεδομένων από κυβερνοεπιθέσεις, τα οποία έχουν csv μορφή και έχουν χαρακτηριστικά δικτύων, όπως το πλήθος το πακέτων που μεταφέρθηκαν και ο όγκος δεδομένων, καθώς και η ετικέτα ταξινόμησης, η οποία δηλώνει εάν υπάρχει εισβολή και, σε περίπτωση που υπάρχει, το είδος αυτής. Σχετικά με τη μεθοδολογία, σε πρώτο στάδιο, γίνεται η επιλογή συνόλου δεδομένων που θα χρησιμοποιηθεί. Το σύνολο αυτό έχει χαρακτηριστικά που σχετίζονται με δεδομένα δικτύου καθώς και χαρακτηριστικό που αφορά την ταξινόμηση. Για τα επιμέρους csv αρχεία δεδομένων (καθώς κάθε σύνολο δεδομένων μπορεί να περιέχει πολλά csv επιμέρους αρχεία), αναλύονται τα κοινά τους χαρακτηριστικά και σε δεύτερο στάδιο, αναφέρεται ο τρόπος χρήσης των αρχειών αυτών. Σε τρίτο στάδιο, γίνεται η επεξεργασία, η εκπαίδευση και η αξιολόγηση των αποτελεσμάτων. Σχετικά με τους αλγορίθμους, εξετάστηκαν οι αλγόριθμοι μηχανικής μάθησης Gaussian Naive Bayes, K Nearest Neighbors, Decision Tree, Random Forest, Multilayer Perceptron (MLP), Logistic Regression και Support-Vector Machine (SVM), στο πλαίσιο της ταξινόμησης (classification). Η οργάνωση της διπλωματικής εργασίας είναι τέτοια ώστε να περιγράφονται αρχικά τα συστήματα και τα σύνολα δεδομένων, έπειτα η μεθοδολογία και οι αλγόριθμοι που χρησιμοποιήθηκαν, και τέλος τα αποτελέσματα που εκμαιεύονται. Για την ακρίβεια, στο τρίτο κεφάλαιο αναφέρεται η μεθοδολογία και οι αλγόριθμοι μηχανικής μάθησης, και στο τέταρτο κεφάλαιο αναφέρονται τα αποτελέσματα καθώς και ο σχολιασμός αυτών.

Ως εκ τούτου, στη διπλωματική εργασία γίνεται η μελέτη των συνόλων δεδομένων που υπάρχουν, τα οποία μπορούν να χρησιμοποιηθούν με σκοπό την εκπαίδευση μοντέλων και απώτερο στόχο την κάλυψη του προβλήματος της ανίχνευσης εισβολών.

Κεφάλαιο 2: Επισκόπηση συστημάτων ανίχνευσης εισβολών και συνόλων δεδομένων

2.1 Βασικές αρχές των συστημάτων ανίχνευσης εισβολών

Στο κεφάλαιο αυτό θα περιγράψουμε τις βασικές αρχές των υπολογιστικών συστημάτων ασφαλείας (computer security systems) που αφορούν την ανίχνευση εισβολών και τον τρόπο λειτουργίας τους [7][8]. Με την έννοια εισβολή εννοούμε την μη εξουσιοδοτημένη πράξη παράκαμψης αρχών ασφαλείας σχετικά με τους μηχανισμούς ενός συστήματος.

Ένα σύστημα εντοπισμού παραβίασης (IDS) στην πράξη αποτελείται από 3 συστατικά (components):

Αισθητήρες (sensors): Σκοπός των αισθητήρων είναι να συλλέγουν δεδομένα. Η είσοδος ενός αισθητήρα μπορεί να είναι οποιοδήποτε τμήμα του συστήματος που είναι επιρρεπές σε παραβίαση. Οι τύποι εισόδου αισθητήρα μπορεί να είναι διαφόρων ειδών, όπως δικτυακά πακέτα (network packages), αρχεία καταγραφής (log files) και ίχνη συστημικών κλήσεων (system call traces). Τα δεδομένα που συλλέγονται από την έξοδο του αισθητήρα προωθούνται στον αναλυτή.

Αναλυτές (analyzers): Σκοπός των αναλυτών είναι να καθορίσουν εάν έχει συμβεί εισβολή. Δέχονται στην είσοδο τους δεδομένα από έναν ή και περισσότερους αισθητήρες ή και από άλλους αναλυτές. Τα δεδομένα εισόδου των αναλυτών μπορούν να αποθηκευτούν σε κάποιο σύστημα ή σε βάση δεδομένων με σκοπό μελλοντική ανάλυση, χρήση και αξιολόγηση. Η έξοδος του αναλυτή είναι ένας δείκτης (indicator) που δηλώνει το συμβάν της παραβίασης. Ορισμένοι αναλυτές παρέχουν καθοδήγηση για πράξεις που μπορούν να γίνουν με σκοπό να μετριάσουν τις αρνητικές επιπτώσεις.

Διεπαφή χρήστη (user interface): Σκοπός του UI ενός IDS είναι η δυνατότητα στον χρήστη να δει την έξοδο από ένα σύστημα καθώς και να ελέγξει τη συμπεριφορά του συστήματος αυτού. Σε κάποια συστήματα, το UI μπορεί να είναι μία συνιστώσα τύπου manager, director ή και console.

Ένα απλό IDS μπορεί να χρησιμοποιεί έναν μόνο αισθητήρα, και έναν μόνο αναλυτή. Παραδείγματα αυτού είναι ένα HIDS σε έναν host ή και ένα NIDS σε μία συσκευή firewall.

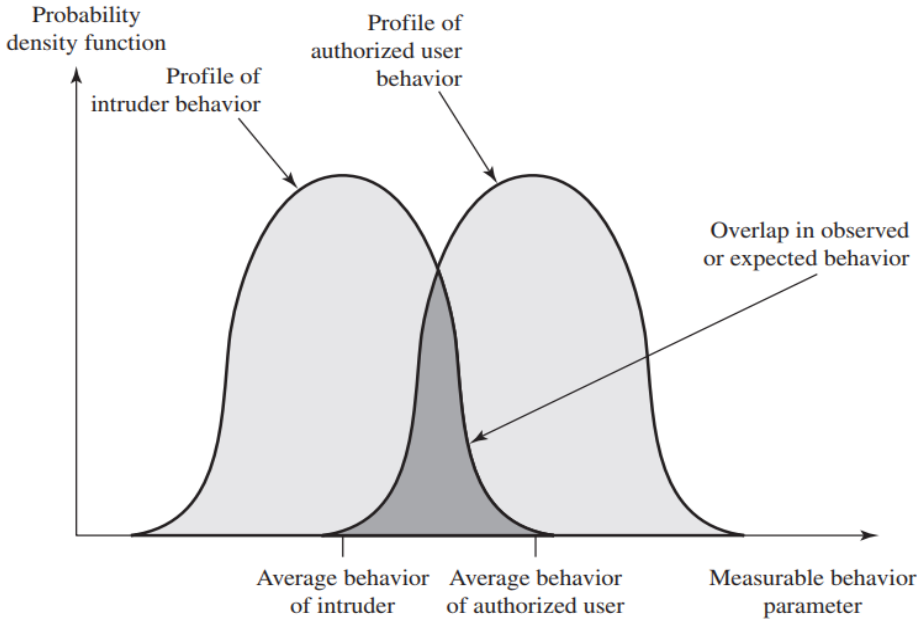
Ένα πιο σύνθετο IDS μπορεί να έχει πολλούς αισθητήρες, σε ένα πλήθος από συσκευές hosts και networks. Στην περίπτωση αυτή, υπάρχει ένας συγκεντρωτικός αναλυτής (centralized analyzer).

Τα IDS ταξινομούνται ανάλογα το source και τον τύπο του αναλυτή, σε Host-based IDS (HIDS), Network-based IDS (NIDS) και κατανεμημένα/υβριδικά (distributed/hybrid) IDS. Τα Host-based IDS (HIDS) παρακολουθούν τα χαρακτηριστικά ενός host καθώς και τα γεγονότα που συμβαίνουν στον host αυτόν (όπως process identifiers ή τα system calls που γίνονται) ώστε να εντοπίσουν ύποπτη δραστηριότητα. Τα Network-based IDS (NIDS) παρακολουθούν την κίνηση δικτύου σε συγκεκριμένα σημεία ή συσκευές και αναλύουν τα (κατά OSI layers ορισμό) πρωτόκολλα δικτύου (network), μεταφοράς (transport) και εφαρμογής (application), ώστε να εντοπίσουν ύποπτη δραστηριότητα. Τα κατανεμημένα/υβριδικά IDS συνδυάζουν host-based και network-based πληροφορίες από πολλούς αισθητήρες σε έναν συγκεντρωτικό αναλυτή.

Για την αναγνώριση παραβίασης, σημαντικό ρόλο παίζουν οι λειτουργίες που έχουν σχέση με αυθεντικοποίηση (authentication), με έλεγχο πρόσβασης (access control) και με firewalls. Όσο νωρίτερα βρεθεί η παραβίαση τόσο μικρότερη η βλάβη από αυτή. Ένα IDS μπορεί να αποτρέπει παραβιάσεις μέσω του έγκαιρου εντοπισμού τους, καθώς και να συλλέγει πληροφορίες για τις τεχνικές παραβίασης με σκοπό να ενδυναμώσει τα μέτρα προστασίας από παραβίαση.

Πρακτικά η αναγνώριση παραβίασης υποθέτει πως υπάρχει διαφορετική συμπεριφορά του εισβολέα χρήστη σε σχέση με έναν που συμπεριφέρεται έγκυρα. Η διαφορετική συμπεριφορά αυτή πρέπει να είναι ποσοτικοποιημένη. Παρόλα αυτά, και ο εισβολέας χρήστης και ο έγκυρος χρήστης, έχουν συμπεριφορά και με διαφορετικά αλλά και με κοινά στοιχεία. Σε περίπτωση μετάφρασης της συμπεριφοράς εισβολής ως έγκυρη, τότε οι υπόλοιποι αντίστοιχοι εισβολείς θα μεταφράζονται επίσης ως έγκυροι και το αποτέλεσμα είναι να έχουμε ψευδώς θετικά (false

positive) αποτελέσματα. Σε περίπτωση μετάφρασης της μη εισβολής ως εισβολή, υπάρχουν αποτελέσματα ψευδώς αρνητικά (false negative).



Εικόνα 1: Προφίλ συμπεριφοράς των χρηστών εισβολέων και μη.

Στην πράξη ένα IDS οφείλει να έχει υψηλό βαθμό ανίχνευσης των συνολικών επιθέσεων ώστε να υπάρχει ελαχιστοποίηση των ψευδώς θετικών και ψευδώς αρνητικών αποτελεσμάτων. Για να γίνει αυτό, χρησιμοποιείται αναγνώριση προτύπων (patterns recognition). Πρακτικά δηλαδή, γίνεται αναγνώριση σχετικά με το παρελθόν της δραστηριότητας, και έτσι προκύπτει ο βαθμός απόκλισης με βάση το κατά πόσο υπάρχει σημαντική απόκλιση με βάση κάποια πρότυπα.

2.2 Συστήματα ανίχνευσης εισβολών και σύνολα δεδομένων

Στο σημείο αυτό, παρουσιάζονται επιλεγμένα συστήματα ανίχνευσης εισβολών καθώς και σύνολα δεδομένων. Τα παρακάτω συστήματα ανίχνευσης εισβολών έχουν επιλεχθεί για ανασκόπηση καθώς είναι τα πιο δημοφιλή. Κύριο επίσης κριτήριο είναι το ότι εξετάζονται HIDS και NIDS συστήματα (και κατανεμημένα/υβριδικά σε περίπτωση που ένα σύστημα πληρεί και HIDS και NIDS λειτουργικότητες).

2.2.1 Συστήματα ανίχνευσης εισβολών

2.2.1.1 Snort

Το Snort είναι ένα NIDS freeware εργαλείο. Είναι διαθέσιμο σε Windows, Linux, Fedora, Centos και FreeBSD και διατηρείται από τη Cisco Systems. Μπορεί να ρυθμιστεί ώστε να παρακολουθεί και να αναλύει την κίνηση δικτύου σε πραγματικό χρόνο για απόπειρες εισβολής, να την καταγράφει και να κάνει μια συγκεκριμένη ενέργεια όταν ανιχνεύεται μια προσπάθεια εισβολής όπως υπερχείλιση προσωρινής μνήμης (buffer overflow), κρυφό σκανάρισμα θύρας (stealth port scan), επίθεση τύπου κοινής διεπαφής πύλης (CGI attack) και αναγνώριση αποτυπώματος λειτουργικού συστήματος (OS fingerprinting). Είναι ένα από τα πιο ευρέως διαδεδομένα εργαλεία IDS και λειτουργεί επίσης ως σύστημα εμπόδισης εισβολής (IPS). Το Snort είναι το παλαιότερο IDS έχοντας ενεργή κοινότητα που παρέχει πλήρη υποστήριξη, κάτι που βοηθάει τους προγραμματιστές.

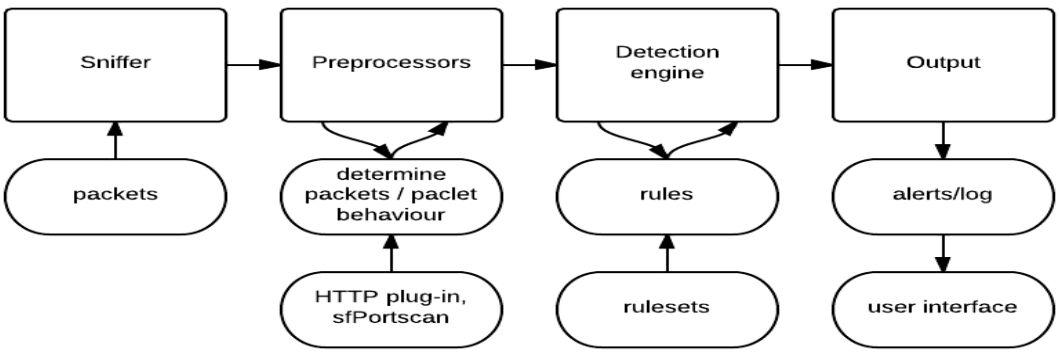
Το Snort έχει ευρεία παραμετροποίηση και γι αυτό το χρησιμοποιούν πολλοί οργανισμοί. Ισχυρή εναλλακτική του Snort είναι το Suricata. Αν και τα δύο αυτά NIDS είναι γραμμένα σε C, το Snort διαφέρει με κύριο χαρακτηριστικό από το Suricata στο ότι το πρώτο είναι μονονηματικό (single-threaded), ενώ το δεύτερο είναι πολυνηματικό (multi-threaded).

Το Snort λειτουργεί σε τρεις διαφορετικές λειτουργίες: sniffer mode, packet logger, intrusion detection. Η λειτουργία ανίχνευσης εισβολών βασίζεται σε αυτό που ονομάζεται «βασικές πολιτικές», οι οποίες είναι πρακτικά ένα σύνολο κανόνων. Μπορούν να προστεθούν εξατομικευμένοι κανόνες ή να χρησιμοποιηθούν οι κανόνες που αναπτύχθηκαν και κοινοποιήθηκαν από την κοινότητα Snort. Για παράδειγμα [75], υπάρχει το αρχείο “snort.conf”, στο οποίο γίνεται να οριστεί ως μεταβλητή μία IP διεύθυνση με σκοπό να προστατευτεί. Στην περίπτωση αυτή, θέτοντας στο αρχείο αυτό την εντολή “ipvar HOME_NET 192.162.132.0/24”, ορίζεται η τοπική διεύθυνση. Έχοντας ορίσει ως κανόνα την πρόσβαση σε τοπική διεύθυνση, έπειτα με την εντολή “sudo snort -A console -q -c /etc/snort/snort.conf -i eht0” απεικονίζονται τα alerts στην κονσόλα του χρήστη. Σε περίπτωση που εκτελεστεί η εντολή “ping 192.168.x.x”, τότε θα προκύψει ειδοποίηση στο πρόγραμμα Snort καθώς το alert ανήκει στους κανόνες που έχουν φορτωθεί.

Μπορούμε να ρυθμίσουμε το snort προκειμένου να εφαρμοστούν είτε signature based είτε anomaly based τεχνικές: Οι signature based και οι anomaly based ανιχνεύσεις είναι οι δύο κύριες μέθοδοι για την ανίχνευση και αναφορά εισβολών. Οι μέθοδοι ανίχνευσης τύπου signature based χρησιμοποιούνται για γνωστές απειλές, ενώ οι μέθοδοι anomaly based χρησιμοποιούνται για αλλαγές στην συμπεριφορά. Ένα παράδειγμα ρύθμισης του Snort για signature based λειτουργία αποτελεί η ρύθμισή του για αναγνώριση πακέτων δεδομένων που ήδη είναι γνωστά ή ορίζοντας μία λίστα από IP διευθύνσεις ως κακόβουλη στα rules του Snort. Από την άλλη, ένα παράδειγμα ρύθμισης του Snort για anomaly based λειτουργία [77][78][43][55][21], είναι να χρησιμοποιηθούν αλγόριθμοι μηχανικής εκμάθησης με σκοπό να δημιουργηθούν κανόνες ταξινόμησης (classification rules) [76]. Η ενέργεια αυτή αποσκοπεί στην επιλογή κατάλληλων χαρακτηριστικών ή βέλτιστων παραμέτρων στο πλαίσιο της διαδικασίας ανίχνευσης εισβολών.

Το Snort έχει κάποια μειονεκτήματα. Το GUI δεν είναι φιλικό, παρόλο που δημιουργήθηκαν γραφικά περιβάλλοντα από την κοινότητα για την επίλυση αυτού του ζητήματος. Λόγω πρακτικής έλλειψης γραφικής διεπαφής χρήστη (GUI) ή κονσόλας διαχείρισης (administrative console), συνήθως χρησιμοποιείται παράλληλα με άλλα εργαλεία ανοιχτού κώδικα όπως τα Snorby, Base, Squil και Anaval για να γεφυρώσουν αυτή την έλλειψη και να να πραγματοποιήσουν εις βάθος ανάλυση των δεδομένων που συλλέγονται από το Snort. Η λειτουργία των πακέτων επεξεργασίας μπορεί να είναι αργή. Όταν δημιουργούνται προσαρμοσμένοι κανόνες ίσως δημιουργούνται και κατά συνέπεια ψευδώς θετικά αποτελέσματα.

Το επόμενο workflow περιγράφει πως λειτουργεί το Snort:



Εικόνα 2: Τρόπος λειτουργίας του Snort.

Στην παραπάνω εικόνα απεικονίζεται ο τρόπος λειτουργίας του προγράμματος Snort. Διαθέσιμα πακέτα γίνονται sniff και έπειτα επεξεργάζονται καθώς καθορίζεται η συμπεριφορά τους. Στη συνέχεια γίνεται η ανίχνευση βάσει προκαθορισμένων κανόνων που έχουν οριστεί. Η έξοδος του συστήματος είναι log αρχεία τα οποία μπορούν να αποτελούν είσοδο σε εφαρμογές ανάγνωσης τέτοιων αρχείων.

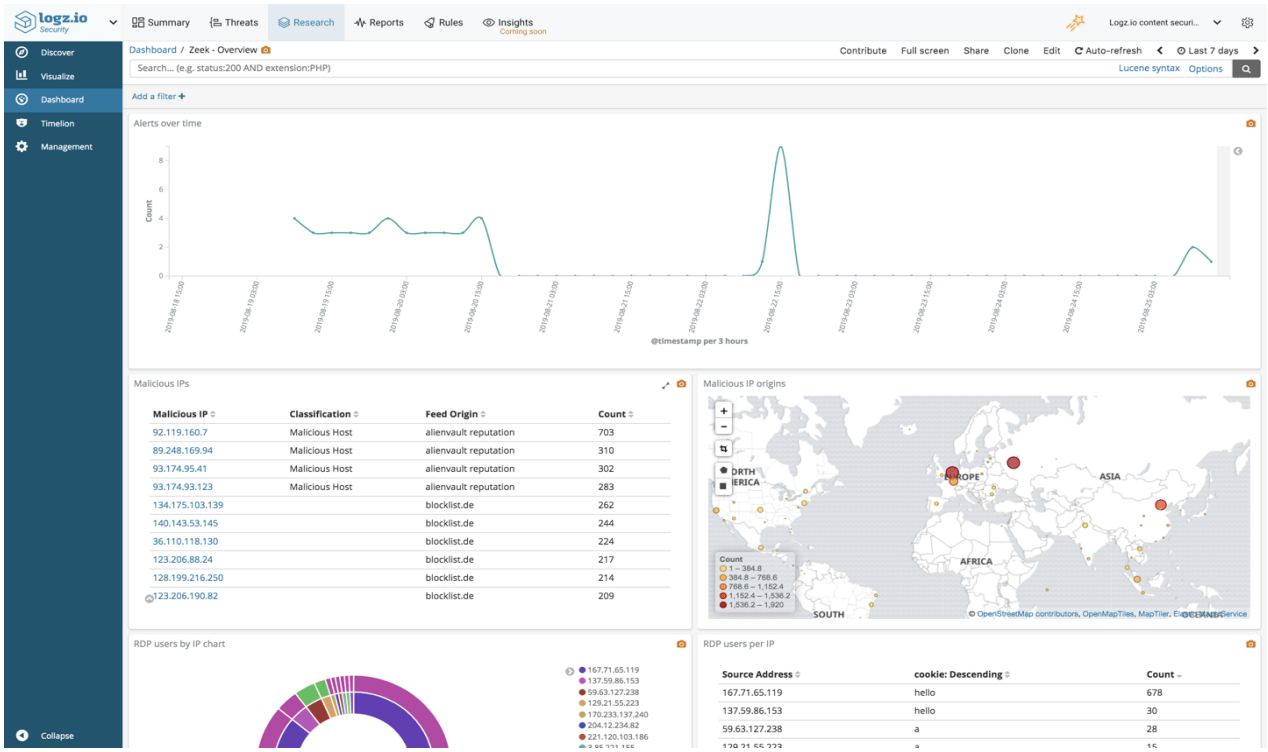
2.2.1.2 Zeek (Bro)

Το Zeek είναι ένα freeware εργαλείο NIDS ανοιχτού κώδικα που επικεντρώνεται σε ανάλυση γενικής κίνησης. Χρησιμοποιεί μία domain-specific γλώσσα που δεν στηρίζεται σε παραδοσιακές υπογραφές. Αυτό δίνει τη δυνατότητα για σχεδιασμό εργασιών για την εκάστοτε policy engine. Για παράδειγμα, το εργαλείο αυτό ρυθμίζεται για να χρησιμοποιεί ύποπτα αρχεία, στέλνοντάς τα για ανάλυση, και να ειδοποιεί σχετικές αρχές για πιθανή απόπειρα εισβολής. Επίσης μπορεί να θέσει σε μαύρη λίστα κώδικα προγραμματισμού και να τερματίσει μία συσκευή που κάνει μεταφόρτωση. Το Zeek λειτουργεί στα λειτουργικά συστήματα Unix/ Linux, Free BSD, και Mac OS X και ανιχνεύει ύποπτες υπογραφές (signatures) και ανωμαλίες (anomalies). Η κοινότητα του Zeek υποστηρίζεται πανεπιστημιακούς φορείς, supercomputing κέντρα, ερευνητικά εργαστήρια και διάφορες άλλες σχετικές κοινότητες.

Έχει τις λειτουργίες first traffic logging, managed by an event engine και analysis. Η διαφορά του με το Snort είναι ότι τρέχει επίσης και στο επίπεδο εφαρμογής, άρα μπορεί να ιχνηλατήσει services σχετικά με HTTP, DNS, SNMP, και FTP, χρησιμοποιώντας ειδικούς αναλυτές. Όπως και τα υπόλοιπα αντίστοιχα NIDS εργαλεία, έτσι και το Zeek, καθώς χρησιμοποιεί signature based και anomaly based detection τεχνικές, παρακολουθεί πακέτα που μεταφέρονται στο δίκτυο και τα συγκρίνει με γνωστά μηνύματα σε βάσεις δεδομένων σημειώνοντας έτσι ύποπτη συμπεριφορά (signature based συμπεριφορά), όπως επίσης ειδοποιεί για άγνωστες ύποπτες ενέργειες (anomaly based συμπεριφορά).

Το μειονέκτημά του είναι πως απαιτείται καλή scripting γνώση για να το χειριστεί καποιος. Μπορεί να χρησιμοποιηθεί το Bro-Script ώστε να αυτοματοποιηθεί μέρος της αντίστοιχης εργασίας. Μειονέκτημα του Bro είναι ότι υπάρχει μια απότομη καμπύλη εκμάθησης για να εξαχθεί η μεγαλύτερη αξία από την καμπύλη αυτή, και μπορεί να αποδειχθεί περίπλοκη η ρύθμιση.

Ένα παράδειγμα του Zeek dashboard φαίνεται στην επόμενη εικόνα [16]:



Εικόνα 3: Διεπαφή του προγράμματος Zeek σχετικά με ειδοποιήσεις ανίχνευσης εισβολών.

Στην παραπάνω εικόνα αντιστοιχεί ένα παράδειγμα χρήσης του Zeek μέσα από το πρόγραμμα Kibana. Απεικονίζονται μετρήσεις χαρακτηριστικών όπως η source address, το διάγραμμα που αντιστοιχεί σε ποσοστά επαναληψιμότητας των χαρακτηριστικών αυτών, καθώς και IP διευθύνσεις οι οποίες έχουν ταξινομηθεί ως κακόβουλες. Γίνεται επίσης χαρτογράφηση των διευθύνσεων με σκοπό να ανιχνευθούν εισβολές. Το χρονοδιάγραμμα που απεικονίζεται αντιστοιχεί στο πλήθος των alerts στον άξονα του χρόνου. Η συγκεκριμένη καρτέλα αφορά το dashboard του συστήματος, καθώς υπάρχουν και άλλες διαχειριστικού τύπου με σκοπό την παραμετροποίηση του συστήματος και των αποτελεσμάτων.

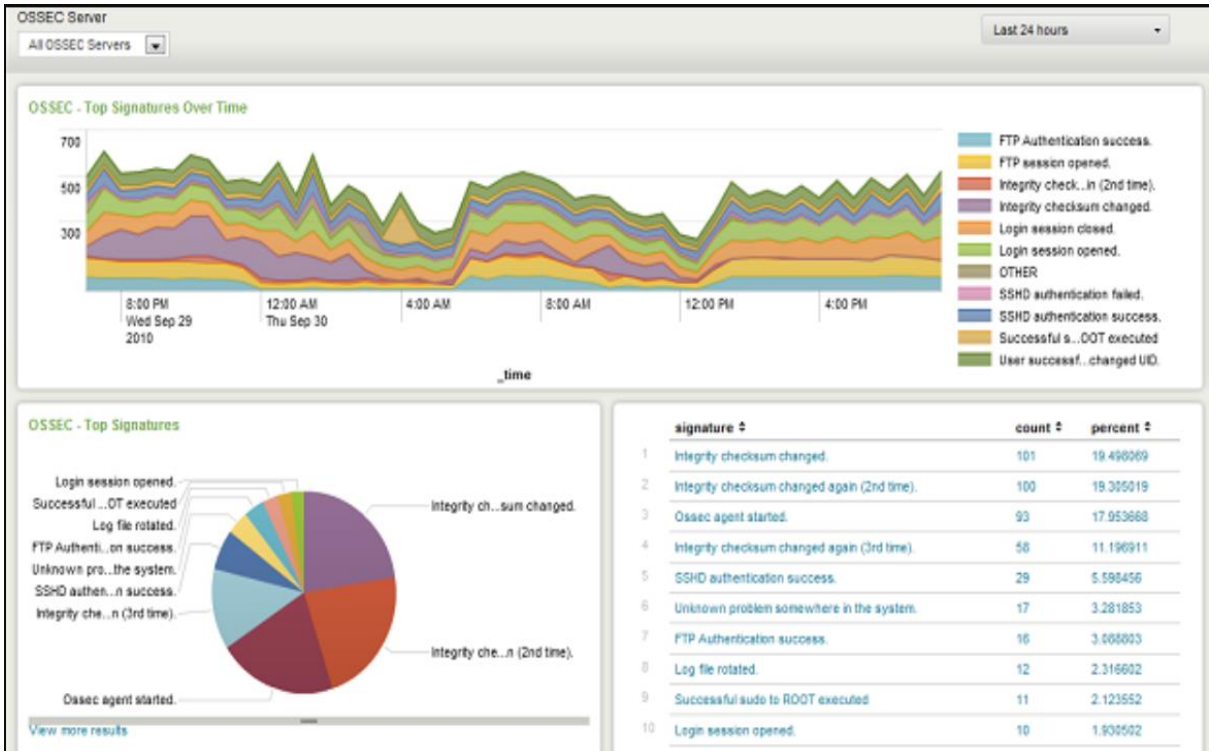
2.2.1.3 OSSEC

Το OSSEC (Open Source HIDS SECurity) είναι ένα επεκτάσιμο ανοιχτού κώδικα HIDS που εκτελεί κυρίως τις λειτουργίες της ανάλυσης αρχείων καταγραφής (log analysis) όπου εξετάζεται ο τύπος και ο όγκος δεδομένων, κυρίως σε συνδυασμό με την ημερομηνία δημιουργίας γεγονότων, την παρακολούθηση της ακεραιότητας αρχείων (file integrity

monitoring) όπου μελετάται κυρίως η μορφολογία των αρχείων, και την παρακολούθηση μητρώου των windows (windows registry monitoring) όπου εξετάζονται κυρίως συστημικές μεταβλητές, και εγγραφές σχετικές με το μητρώο του λειτουργικού συστήματος. Έπονται και άλλες λειτουργίες όπως centralized policy, enforcement, rootkit detection, real-time alerting και active response οι οποίες κατά κύριο λόγο συσχετίζονται με δυναμικές ειδοποιήσεις και απαντήσεις του συστήματος, καθώς και πολιτικές που οφείλουν να τηρούνται σχετικά με την πληροφορία που δρομολογείται (routing) εντός ελεγκτών συστήματος (controllers) και συσκευών.

Το OSSEC εκτελείται σε σχεδόν όλα τα βασικά λειτουργικά συστήματα (Windows, Linux, OpenBSD, FreeBSD, MacOS, Solaris). Έχει την αρχιτεκτονική client - server και στέλνει ειδοποιήσεις (alerts) και αρχεία καταγραφής (logs) σε έναν κεντρικό server για ανάλυση. Αυτή η αρχιτεκτονική γίνεται εύκολα deploy γιατί ο διαχειριστής χρήστης μπορεί να κάνει ενέργειες σε όλους τους agents από έναν μόνο server. Ο OSSEC installer είναι πολύ ελαφρύς (κάτω από 1MB) και καταλαμβάνει λίγα CPU resources κατά τη λειτουργία. Είναι επίσης προσαρμόσιμο και μπορεί να ρυθμιστεί ώστε να λειτουργεί σε πραγματικό χρόνο αυτόματα, και υπάρχει υποστήριξη από μεγάλη κοινότητα. Σε περίπτωση που κάποιος δεν ενδιαφέρεται για κεντρικό υπολογιστή, μπορεί να εξετάσει το Samhain Labs ως μια εναλλακτική λύση που βασίζεται επίσης σε κεντρικό υπολογιστή, αλλά προσφέρει πολλαπλές μεθόδους εξόδου από τον agent.
Με το OSSEC μπορούμε να εφαρμόσουμε πρακτικά δύο ειδών μεθόδους με σκοπό να κάνουμε monitor τα logs [41], οι οποίες είναι αυτές της παρακολούθησης διαδικασιών (Process Monitoring) καθώς και παρακολούθησης αρχείων (File Monitoring). Στην περίπτωση παρακολούθησης διαδικασιών αξιολογούνται οι διαδικασίες του προγράμματος που παρεμβαίνουν (process intervention). Στην περίπτωση παρακολούθησης αρχείων, κυρίως ειδοποιούνται συστημικοί διαχειριστές σχετικά με της αλλαγή, διαγραφή, ή δημιουργία αρχείων στο σύστημα.

Παρακάτω φαίνεται ένα παράδειγμα του OSSEC [17] :



Εικόνα 4: Διεπαφή του προγράμματος OSSEC σχετικά με ειδοποιήσεις ανίχνευσης εισβολών.

Στην παραπάνω εικόνα εμφανίζεται ένα παράδειγμα από το dashboard του συστήματος OSSEC. Εμφανίζεται στον άξονα του χρόνου χάρτης με τα γεγονότα, όπως το επιτυχές Login σε μία εφαρμογή. Επίσης εμφανίζεται το πλήθος των γεγονότων σε καθαρό αριθμό αλλά και σε ποσοστό.

2.2.1.4 Suricata

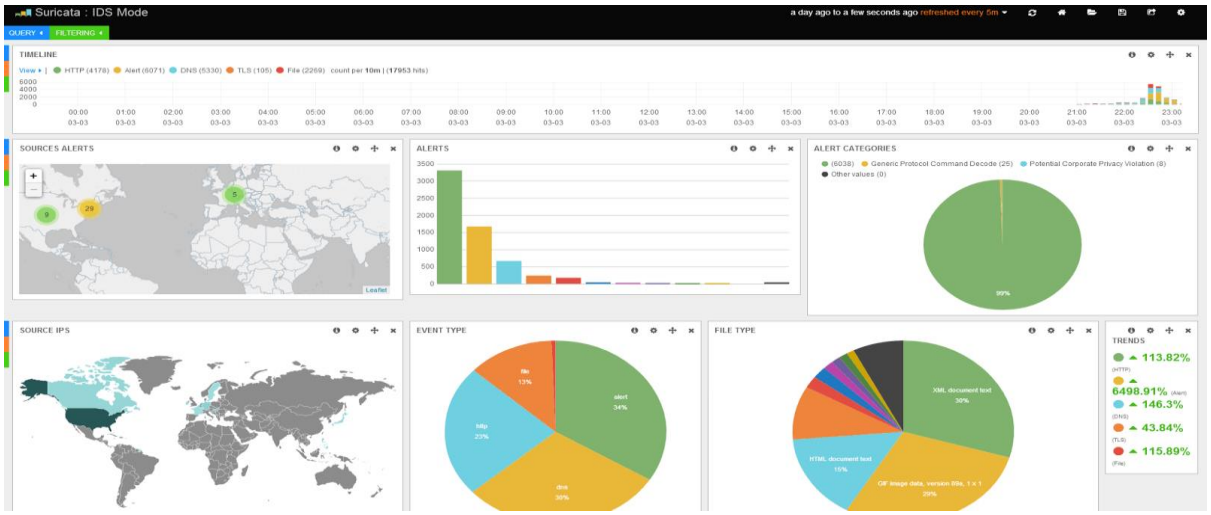
Το Suricata είναι ανοικτού κώδικα NIDS που εκτελεί τις λειτουργίες ανίχνευσης εισβολών σε πραγματικό χρόνο (όπου λαμβάνονται πακέτα από το δίκτυο και έπειτα περνούν σε στάδιο ανάλυσης και επεξεργασίας), inline intrusion prevention (IPS, όπου εξετάζονται ροές δικτυακής κίνησης με σκοπό την ανίχνευση αλλά και αποτροπή κακόβουλων ενεργειών), network security monitoring (NSM, όπου πρακτικά υπολογιστικά services παρακολουθούν το δίκτυο για απειλές και ύποπτες συμπεριφορές) και offline pcap processing. Στην τελευταία περίπτωση, τα δεδομένα αποθηκεύονται σε αρχεία μέσα σε συσκευές υψηλής ταχύτητας

αποθήκευσης (high-speed data storage devices) με σκοπό να επιταχυνθούν οι διαδικασίες εισόδου και εξόδου δεδομένων στους υπολογιστές (data input and output speed up).

Θεωρείται πλήρες σύστημα παρακολούθησης δικτύου. Δεν έχει την αρχιτεκτονική του Snort αλλά συμπεριφέρεται σαν αυτό και χρησιμοποιεί τις ίδιες υπογραφές. Ενώ το Snort είναι μονονηματικό (χρησιμοποιεί ένα CPU at a time), το Suricata είναι πολυνηματικό (χρησιμοποιεί τα διαθέσιμα CPUs). Έχει μία built-in hardware acceleration τεχνολογία που μπορεί να μοχλεύει την ισχύ των γραφικών καρτών με σκοπό την επιθεώρηση της κίνησης δικτύου.

Το Suricata μπορεί να χρησιμοποιήσει Lua scripts που μπορούν να χρησιμοποιηθούν για traffic/decode malware. Είναι διαθέσιμο σε λειτουργικά συστήματα Linux, FreeBSD, OpenBSD, macOS / Mac OS X, και Windows, και έχει υποστηρικτική κοινότητα. Αυτό το σύστημα μπορεί να κάνει ανίχνευση εισβολών στο δίκτυο στην εξέταση πιστοποιητικών TLS, αιτημάτων HTTP και συναλλαγών DNS. Για να εξασφαλίσει αποδοτική ενσωμάτωση με άλλες τεχνικές λύσεις, όπως SIEM και βάσεις δεδομένων, το Suricata χρησιμοποιεί αρχεία YAML και JSON ως εισόδους και εξόδους.

Η επόμενη εικόνα εμφανίζει ένα ενδεικτικό Suricata dashboard σε κατάσταση ανίχνευσης εισβολών:



Εικόνα 5: Διεπαφή του προγράμματος Suricata σχετικά με ειδοποιήσεις ανίχνευσης εισβολών.

Στην παραπάνω εικόνα εμφανίζεται ένα ενδεικτικό παράδειγμα της χρήσης του προγράμματος Suricata. Αναγνωρίζεται στον άξονα του χρόνου (ημέρα, ώρα) το είδος του γεγονότος, όπως alert, όπως http, tls, file και dns. Εμφανίζονται επίσης διαγράμματα με το πλήθος των ειδοποιήσεων και διευθύνσεις IP σε χάρτη παγκοσμίως, ποσοστιαίες απεικονίσεις των τύπων γεγονότων, οι τύποι αρχείων που αντιστοιχούν σε γεγονότα καθώς και οι κατηγορίες των πιθανών εισβολών.

2.2.1.5 Security Onion

Το Security Onion είναι ένα ανοικτού κώδικα NIDS εργαλείο με τις λειτουργίες κυνηγιού απειλής (threat hunting), ανίχνευσης εισβολών, παρακολούθησης επιχειρησιακής ασφάλειας (enterprise security monitoring) και διαχείρισης αρχείων καταγραφής (log management). Στην περίπτωση του κυνηγιού απειλής εκτελούνται διαδικασίες πρόληψης και επαναληπτικής αναζήτησης μέσω δικτύων για τον εντοπισμό και την απομόνωση προηγούμενων απειλών. Στην περίπτωση της παρακολούθησης επιχειρησιακής ασφάλειας, ακολουθούνται ορισμένα πρότυπα ασφαλείας σχετικά με την συστημική ασφάλεια. Υπάρχουν πιστοποιήσεις όπως το ISO 27001, που βοηθούν επιχειρήσεις και οργανισμούς να βελτιώσουν την διαχείριση ασφάλειας μέσω συστημάτων (information security management systems, ISMS) .

Το συγκεκριμένο εργαλείο συνδυάζει εργαλεία εντοπισμού εισβολών όπως τα Snort, Kibana, Zeek, Wazuh, CyberChef, NetworkMiner, Suricata, και Logstash. Αυτό το χαρακτηριστικό το κάνει αρκετά περιεκτικό και πολυχρηστικό, καλύπτοντας έτσι μεγάλο φάσμα των αναγκών στον χώρο του IT security. Είναι μειονέκτημα το ότι έχει πολύπλοκο setup καθώς και το ότι είναι σχετικά δύσκολος ο τρόπος με τον οποίο λειτουργεί με πολλαπλά εργαλεία. Έχοντας έναν καλό wizard, το Security Onion εξομαλύνει τις παραπάνω δυσκολίες. Μειονέκτημα αποτελεί το ότι κάποια εργαλεία έχουν επικαλυπτόμενες λειτουργίες, και κατά συνέπεια, χρησιμοποιώντας κάποιες από αυτές, δεν είναι εύκολη (ή είναι αδύνατη) η χρήση άλλων.

Παρακάτω φαίνεται ένα παράδειγμα του Security Onion dashboard [18]:

Εικόνα 6: Διεπαφή του προγράμματος Security Onion σχετικά με ειδοποιήσεις ανίχνευσης εισβολών.

Στην παραπάνω εικόνα φαίνεται ένα ενδεικτικό παράδειγμα χρήσης του προγράμματος Security Onion. Απεικονίζονται γεγονότα, με σκοπό την παρακολούθηση, όπως η ημερομηνία/ώρα, διευθύνσεις IP και ports, για πακέτα, είτε για το source είτε για το destination της πληροφορίας.

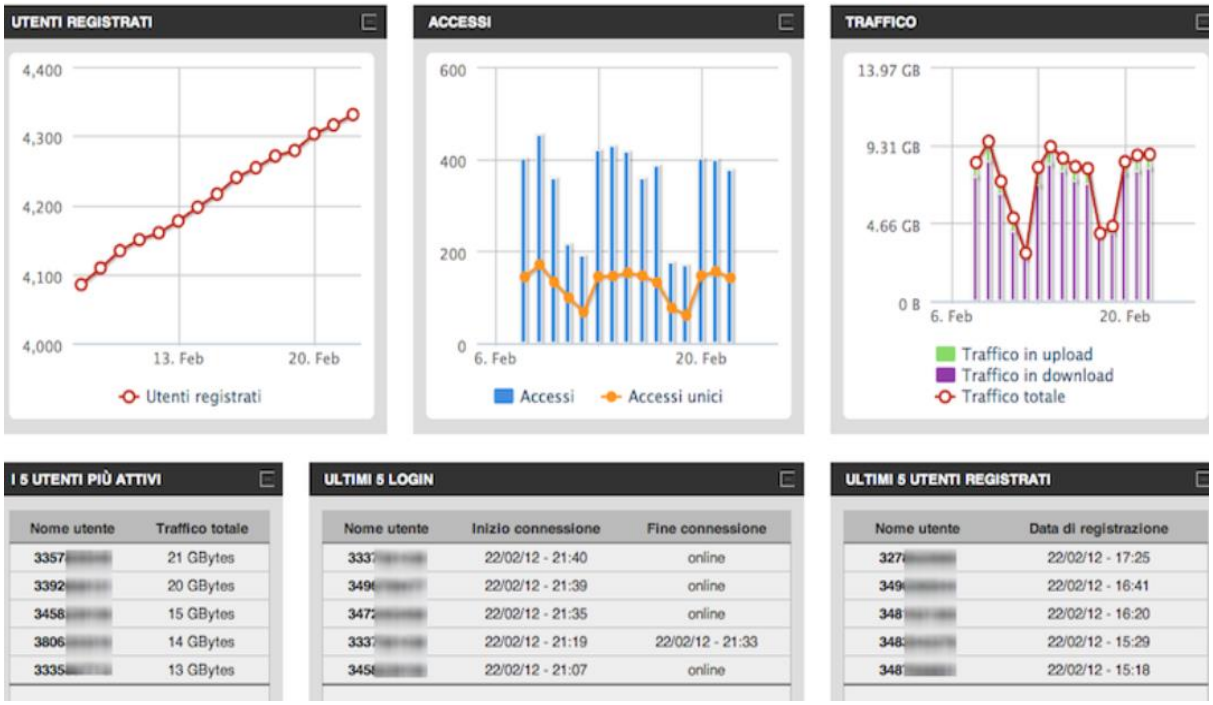
2.2.1.6 OpenWIPS-ng

Το OpenWIPS-ng είναι ανοικτού κώδικα NIDS, για ασύρματα δίκτυα (WIPS - wireless intrusion prevention system). Αναπτύχθηκε από την ομάδα που έφτιαξε και το Aircrack-ng NIDS. Χρησιμοποιείται και ως WiFi sniffer πακέτων. Το OpenWIPS-ng δουλεύει σε Linux και έχει 3 βασικά components: έναν αισθητήρα που συλλέγει δεδομένα, και στέλνει εντολές, έναν server (περιέχει και μία analysis engine) καθώς και ένα GUI που εμφανίζει τα γεγονότα και τις ειδοποιήσεις. Το μεγαλύτερο μέρος της επεξεργασίας εκτελείται στον server καθώς τα περισσότερα plugins εκτελούνται εκεί και τα πακέτα συναρμολογούνται εκ νέου επίσης εκεί.

Η επικοινωνία είναι κρυπτογραφημένη εξ ορισμού και διαχειρίζεται από κανάλια τύπου εντολών και δεδομένων. Αυτό το NIDS έχει ορισμένους περιορισμούς. Κάθε εγκατάσταση

περιλαμβάνει μόνο έναν αισθητήρα. Επιπλέον, οι αισθητήρες δεν εντοπίζουν πάντα την ίδια κίνηση.

Παρακάτω φαίνεται ένα παράδειγμα χρήσης του συστήματος OpenWIPS-ng:



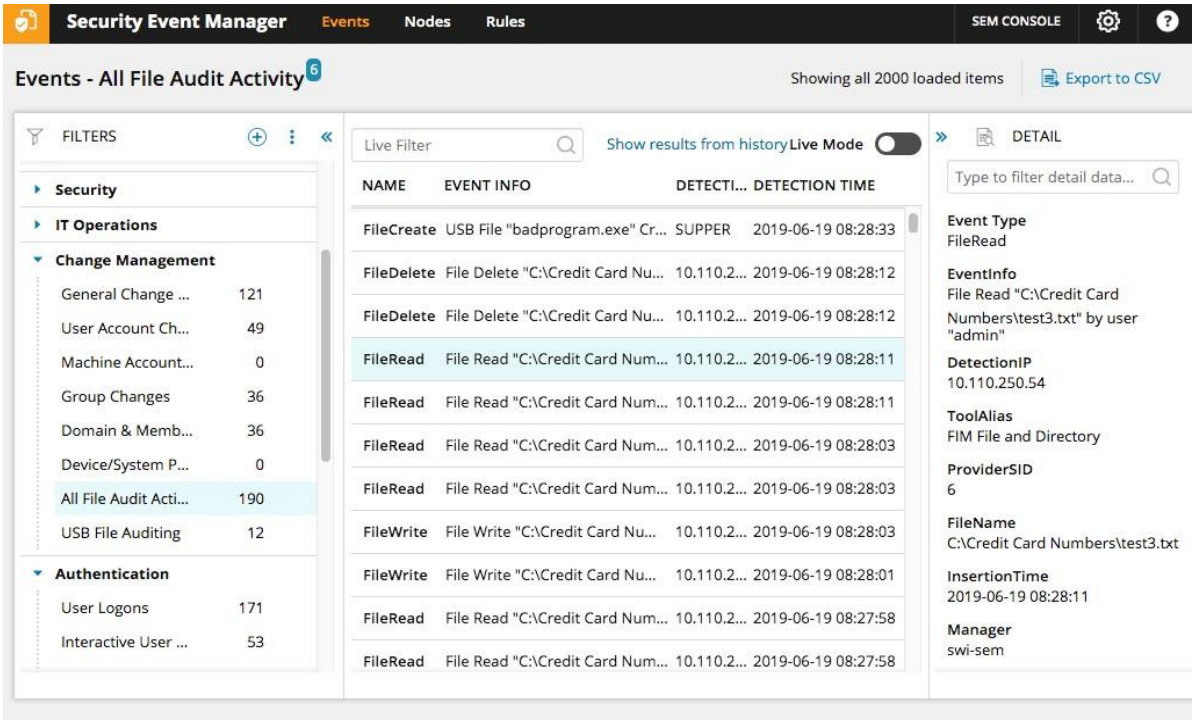
Εικόνα 7: Ενδεικτικό παράδειγμα λειτουργίας του OpenWIPS-ng.

Στην παραπάνω εικόνα εμφανίζονται λειτουργίες του προγράμματος OpenWIPS-ng, και συγκεκριμένα του OpenWCPM (OpenWISP Captive Portal Manager). Απεικονίζονται οι εγγεγραμμένοι χρήστες σε μία εφαρμογή στον άξονα του χρόνου. Φαίνεται η καμπύλη επίσης που δείχνει την πρόσβασή τους, την κίνηση δικτύου σε περιπτώσεις όπως upload και download, καθώς και καταστάσεις του συστήματος όπως ο συνολικός αριθμός των login στην εφαρμογή στον άξονα του χρόνου.

2.2.1.7 SolarWinds Security Event Manager

Το Security Event Manager (SEM) [24] είναι ένα HIDS με αυτοματοποιημένα εργαλεία τύπου threat remediation, το οποίο εν τέλει είναι ένα IPS. Μπορεί να κάνει διαχείριση και παρακολούθηση αρχείων καταγραφής, καθώς και forward, back up, ή archive των αρχείων αυτών. Επίσης περιλαμβάνει κρυπτογραφημένο σύστημα αποθήκευσης.

Παρακάτω φαίνεται ένα SolarWinds Security Event Manager dashboard:



Εικόνα 8: Διεπαφή του προγράμματος SolarWinds Security Event Manager σχετικά με ειδοποιήσεις ανίχνευσης εισβολών.

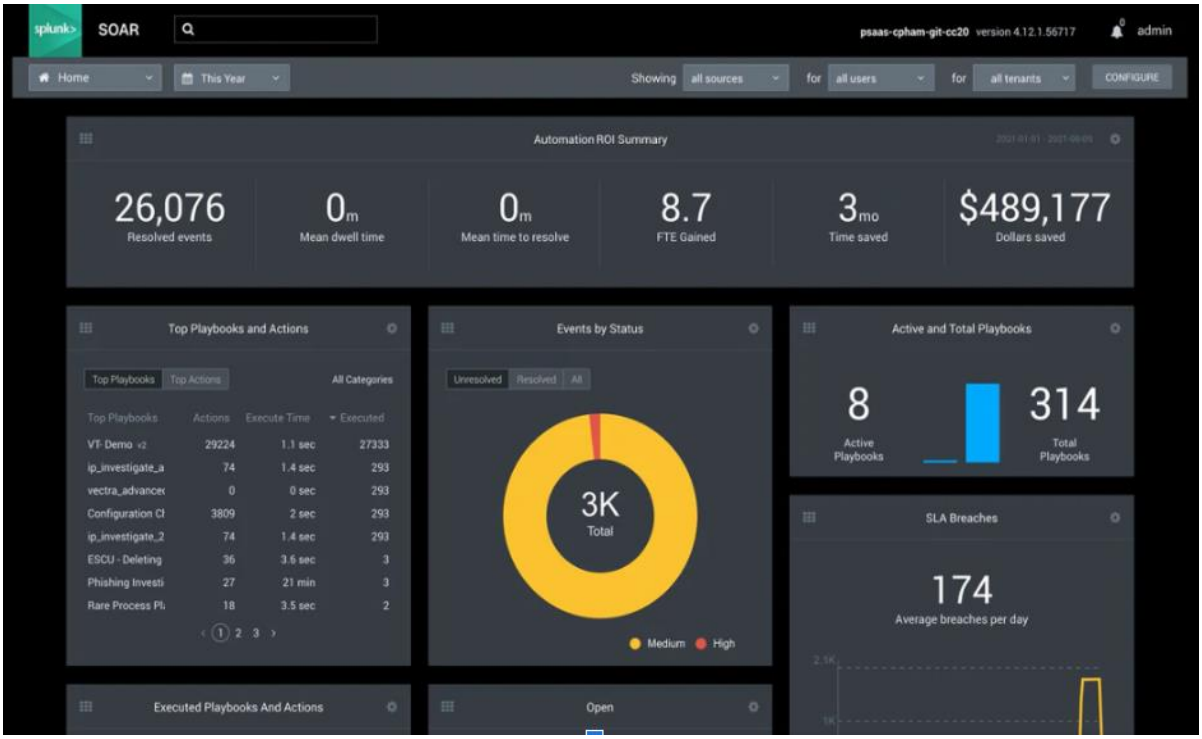
Στην παραπάνω εικόνα φαίνονται για το πρόγραμμα Security Event Manager τα γεγονότα με τις αντίστοιχες ημερομηνίες και ώρες. Απεικονίζεται το όνομα του γεγονότος, ο τύπος αυτού και πληροφορίες όπως τα ονόματα αρχείων που μεταφέρθηκαν. Δίνεται η δυνατότητα στον χρήστη του Security Event Manager για εξαγωγή των αρχείων σε CSV μορφή καθώς και η δυνατότητα για παραμετροποίηση του συστήματος.

2.2.1.8 Splunk

Το Splunk [24] έχει διάφορες εκδόσεις, από δωρεάν που αντιστοιχούν σε anomaly based HIDS εώς και επί πληρωμή εκδόσεις NIDS χαρακτηριστικών. Οι δεύτερες συμπεριλαμβάνουν επιλογές cloud, προσφέροντας αυτοματοποιημένα χαρακτηριστικά για αυτόματες γρήγορες απαντήσεις στο πλαίσιο της ανίχνευσης εισβολών. Έτσι, υπάρχουν IPS δυνατότητες και GUI.

Όλες οι εκδόσεις του Splunk μπορούν να εγκατασταθούν σε Windows, Linux, και Mac. Κάθε μία από αυτές περιλαμβάνει έναν δυνατό αναλυτή δεδομένων με σκοπό την εύκολη ταξινόμηση και εύρεση μέσα από δεδομένα στα αρχεία καταγραφής. Υπάρχουν διαφορετικές διαθέσιμες δωρεάν περίοδοι χρήσης του προγράμματος.

Παρακάτω φαίνεται ένα παράδειγμα του Splunk dashboard:



Εικόνα 9: Διεπαφή του προγράμματος Splunk σχετικά με ειδοποιήσεις ανίχνευσης εισβολών.

Στην παραπάνω εικόνα φαίνονται τα γεγονότα που έχουν καταγραφεί με βάση συγκεκριμένα κριτήρια. Εμφανίζεται το dashboard με τον τύπο των γεγονότων, καθώς και η ποσοστιαία κατάσταση που περιγράφει πόσα από αυτά είναι επιλυμένα ή όχι από τον χρήστη που παρακολουθεί το πρόγραμμα Splunk. Απεικονίζονται οι κατά μέσο όρο παραβιάσεις ανά ημέρα, καθώς και φίλτρα που μπορούν να χρησιμοποιηθούν με σκοπό την απομόνωση συγκεκριμένων γεγονότων με βάση ορισμένα κριτήρια.

2.2.2 Συγκριτικός πίνακας συστημάτων ανίχνευσης εισβολών:

Λίστα Συστημάτων Ανίχνευσης Εισβολών			
#	**Σύστημα**	**HIDS**	**NIDS**
1	Snort	×	✓
2	Zeek (Bro)	×	✓
3	OSSEC	✓	×
4	Suricata	✓	×
5	Security Onion	×	✓
6	OpenWIPS-ng	×	✓
7	SolarWinds Security Event Manager (SEM)	✓	×
8	Splunk	✓	✓

Πίνακας 1: Λίστα με συστήματα ανίχνευσης εισβολών και οι διαθέσιμοι τρόποι λειτουργίας τους.

2.3 Σύνολα δεδομένων ανίχνευσης εισβολών

Στο πλαίσιο της διπλωματικής αυτής εργασίας έχουν βρεθεί και αναλυθεί τα παρακάτω σύνολα δεδομένων. Βασικό κριτήριο για την ανάλυση αυτή είναι το πόσο δημοφιλή είναι. Ο επόμενος πίνακας απεικονίζει τα είδη των εισβολών που αναφέρονται στις εγγραφές των συνόλων αυτών δεδομένων.

Είδος εισβολής	**Περιγραφή**
Probe/Data type probing	Η probe επίθεση είναι επεμβατική, αφορά την παράκαμψη μέτρων ασφαλείας παρατηρώντας την φυσική εφαρμογή του chip (physical silicon implementation of a chip). Στην περίπτωση του data type probing, αφορά κακόβουλο node που γράφει διαφορετικούς τύπους δεδομένων αντί του επιθυμητού.
Wrong setup	Εσφαλμένος τρόπος εγκατάστασης hardware / software.
Smurf	Είδος επίθεσης άρνησης εξυπηρέτησης [37].
Worms: Blaster/ Code Red/ Reaper	Κακόβουλο πρόγραμμα υπολογιστή που αναπαράγεται μόνο του με σκοπό να απλωθεί σε άλλους υπολογιστές.
Spam Bot Detection/ Botnet	Πρόγραμμα που αυτοματοποιημένα στέλνει εντολές/διαδικασίες όπως απαντήσεις/email/πληροφορίες χρηστών.
Port Scan/ Service Scan/ Spread	Κακόβουλες επιθέσεις που αφορούν συλλογή πληροφορίας δικτύου/συσκευών πριν την επίθεση. Συνήθως οι τεχνικές scanning συλλέγουν πληροφορίες όπως IP διευθύνσεις/ Ports και εκδόσεις υπηρεσιών.
IP fragmentation/ Packet Fragmentation	Ο κατακερματισμός αντιστοιχεί σε επιθέσεις σχετικές με την ασφάλεια και τον τρόπο που το Internet Protocol (IP) απαιτεί δεδομένα/πακέτα δεδομένων για μεταφορά/επεξεργασία.
Data exfiltration	Η διήθηση/εξώθηση/διείσδυση δεδομένων συμβαίνει όταν κακόβουλο λογισμικό ή/και κακόβουλος παράγοντας πραγματοποιεί μη εξουσιοδοτημένη μεταφορά δεδομένων από υπολογιστή [23].
Keylogging	Αφορά την καταγραφή πληκτρολόγησης, η οποία γίνεται εν αγνοία του χρήστη που πληκτρολογεί.
OS (Operating Systems)	Ο εισβολέας ψάχνει για πρόσβαση στο σύστημα/δίκτυο προσπαθώντας να ανιχνεύσει ευάλωτα σημεία (όπως ανοιχτά ports, services).
DDoS: ICMP/UDP/TCP SYN/HTTP-Flood	Επιθέσεις τύπου DDoS (επίθεση άρνησης υπηρεσιών) σε επίπεδο πρωτοκόλλου ICMP/UDP/TCP/HTTP αντίστοιχα. Οι επιθέσεις DDoS είναι γρηγορότερες των DoS.
DoS/LAND Attack	Επιθέσεις με σκοπό να μη μπορεί ένα service ή ένας υπολογιστής να δεχθεί συνδέσεις. Η Land επίθεση αφορά συγκεκριμένα την περίπτωση όπου κατά την επίθεση τίθεται σε TCP επίπεδο ίδια η πληροφορία για source

	και destination.
U2R (User to Root)	Επιθέσεις εκμετάλλευσης όπου ο εισβολέας ξεκινάει δραστηριότητες σε ένα σύστημα ως απλός χρήστης και στη συνέχεια προσπαθεί να αποκτήσει έλεγχο ως διαχειριστής/super user.
R2L (Remote to user)	Επιθέσεις που αφορούν δίκτυα, και ο εισβολέας στέλνει πληροφορία σε πακέτα σε άλλον υπολογιστή/server μέσω δικτύου στο οποίο δεν έχει δικαιώματα πρόσβασης σας τοπικός χρήστης.
Brute Force FTP	Εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα [48] σχετικά με αρχεία (FTP, File Transfer Protocol).
Brute Force SSH	Εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα σχετικά με δίκτυο και κρυπτογράφηση (SSH, Secure Shell Protocol) [36].
Heartbleed	Ευαλωτότητα (vulnerability) στην OpenSSL cryptographic βιβλιοθήκη λογισμικού.
Web Attack	Κακόβουλες προσπάθειες σε ιστότοπους όπου ο εισβολέας προσπαθεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικό περιεχόμενο/ πληροφορία.
Infiltration	Μέθοδος επίθεσης όπου ένα σχετικά μικρό κομμάτι κακόβουλου λογισμικού προσπαθεί να προκαλέσει βλάβη/ να εισαχθεί σε έναν υπολογιστή.
Man-in-the-middle: Spoofing	Γίνεται sniff πακέτων μεταξύ gateway και server, κάτι που παραβιάζει την εμπιστευτικότητα προσωπικών δεδομένων.
Man-in-the-middle: Data injection	Γίνεται τροποποίηση πακέτων on-the-fly, κάτι που παραβιάζει την ακεραιότητα δεδομένων.

Πίνακας 2: Είδη εισβολών που παρουσιάζονται στα σύνολα δεδομένων εντός της διπλωματικής εργασίας.

2.3.1 NSL-KDD

Το σύνολο δεδομένων NSL-KDD [33][34] δημιουργήθηκε από το σύνολο δεδομένων KDD99, το οποίο με τη σειρά του δημιουργήθηκε από το σύνολο δεδομένων DARPA [47]. Το βασικό σύνολο δεδομένων DARPA, αποτελείται από dump αρχεία που δεν έχουν επεξεργαστεί (raw

dump files) σχετικά με TCP/IP. Με τη διαδικασία της εξαγωγής χαρακτηριστικών (features extraction) προέκυψε το σύνολο δεδομένων KDD99. Με την απαλοιφή διπλότυπων εγγραφών, μειώθηκε το μέγεθος του συνόλου αυτού και προέκυψε το σύνολο δεδομένων NSL-KDD.

Τα χαρακτηριστικά του συνόλου δεδομένων NSL-KDD είναι 4 τύπων, που αντιστοιχούν σε 4 που αφορούν κατηγορίες (categorical), 6 δυαδικά (binary), 23 διακριτών τιμών (discrete) και 10 συνεχών τιμών (continuous). Τα χαρακτηριστικά αυτά απεικονίζονται στον παρακάτω πίνακα [27]:

Classes:	DoS	Probe	U2R	R2L
Sub-Classes:	• apache2 • back • land • neptune • mailbomb • pod • processtable • smurf • teardrop • udpstorm • worm	• ipsweep • mscan • nmap • portsweep • saint • satan	• buffer_overflow • loadmodule • perl • ps • rootkit • sqlattack • xterm	• ftp_write • guess_passwd • httptunnel • imap • multihop • named • phf • sendmail • Snmpgetattack • spy • snmpguess • warezclient • warezmaster • xlock • xsnoop
Total:	11	6	7	15

Πίνακας 3: Τα χαρακτηριστικά του συνόλου δεδομένων NSL-KDD.

Το σύνολο δεδομένων NSL-KDD είναι ένα δημόσιο σύνολο που λύνει κάποια από τα προβλήματα που κληρονομήθηκαν από το σύνολο δεδομένων KDD99. Η νέα αυτή έκδοση του KDD συνόλου έχει ακόμα όμως κάποια προβλήματα. Μπορεί όμως το σύνολο δεδομένων αυτό να εφαρμοστεί ως αποτελεσματικό σημείο αναφοράς (benchmark) με σκοπό να βοηθήσει στην έρευνα σχετικά με τη σύγκριση διαφόρων μεθόδων ανίχνευσης εισβολών.

Ο αριθμός των εγγραφών στο σύνολο δεδομένων NSL-KDD (στα train και test υποσύνολα) είναι τέτοιος ώστε να μπορούν να εκτελεστούν ικανοποιητικά πειράματα. Ο όγκος δεδομένων αντιστοιχεί σε σχετικά μικρό μέγεθος (π.χ. το KDDTest+.csv αρχείο έχει μέγεθος 6.3Mb, 43 features και 22544 εγγραφές). Οι τύποι επιθέσεων που αντιστοιχούν στο NSL-KDD είναι οι DoS, Probe, U2R και R2L.

Στατιστικά, οι περιττές εγγραφές στο KDD train σύνολο δεδομένων φαίνονται στον παρακάτω πίνακα:

Ταξινόμηση	Αρχικές εγγραφές	Μοναδικές εγγραφές (Non duplicates)	Ρυθμός μείωσης
Επιθέσεις	3,925,650	262,178	93.32%
Μη επιθέσεις	972,781	812,814	16.44%
Σύνολο	4,898,431	1,074,992	78.05%

Πίνακας 4: Εγγραφές στο KDD train σύνολο δεδομένων.

Στατιστικά, οι περιττές εγγραφές στο KDD test σύνολο δεδομένων φαίνονται στον παρακάτω πίνακα:

Ταξινόμηση	Αρχικές εγγραφές	Μοναδικές εγγραφές (Non duplicates)	Ρυθμός μείωσης
Επιθέσεις	250,436	29,378	88.26%
Μη επιθέσεις	60,591	47,911	20.92%
Σύνολο	311,027	77,289	75.15%

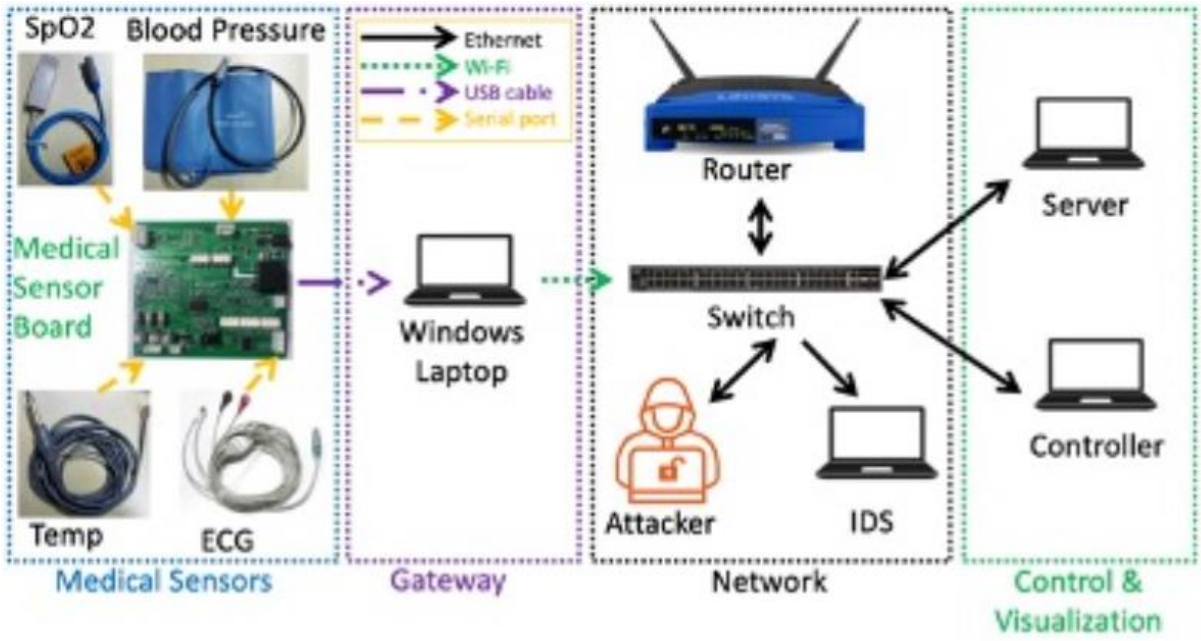
Πίνακας 5: Εγγραφές στο KDD test σύνολο δεδομένων.

2.3.2 WUSTL EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity Research

Το δημόσιο σύνολο δεδομένων αυτό [29][31] δημιουργήθηκε χρησιμοποιώντας σε πραγματικό χρόνο EHMS πλατφόρμα δοκιμών (Enhanced Healthcare Monitoring System testbed) [29], το οποίο πρακτικά συλλέγει μετρικές και από ροές δικτύου καθώς και βιομετρικά δεδομένα ασθενών [30].

Το σύστημα αποτελείται από 4 μέρη, τα οποία είναι οι ιατρικοί αισθητήρες, το gateway, το δίκτυο και ο έλεγχος με οπτικοποίηση. Η ροή δεδομένων ξεκινάει από τους αισθητήρες που είναι τοποθετημένοι στο σώμα του ασθενούς, και καταλήγει στο gateway. Έπειτα, το gateway στέλνει τα δεδομένα στον server, για οπτικοποίηση μέσω switch και router.

Ένας εισβολέας μπορεί να υποκλέψει τα δεδομένα πριν αυτά φτάσουν στον server. Το IDS είναι υπεύθυνο για τη σύλληψη σε πραγματικό χρόνο του flow της κίνησης του δικτύου καθώς και των βιομετρικών δεδομένων του ασθενούς, ειδικά στις περιπτώσεις ανωμαλιών [30]. Τα δεδομένα που αφορούν το δίκτυο, καθώς και τα βιομετρικά δεδομένα, αποθηκεύονται σε αρχεία csv από εργαλείο ARGUS (Audit Record Generation and Utilization System) [31]. Το σύνολο δεδομένων έχει όγκο 4.4 Mb.



Εικόνα 10: Τα τέσσερα μέρη του EHMS Testbed.

Πρακτικά στο σύνολο δεδομένων, οι εγγραφές που αντιστοιχούν σε MAC διεύθυνση υπολογιστή εισβολέα έχουν label 1, ενώ οι υπόλοιπες label 0.

Πρόκειται για συνολικά 16.318 δείγματα, τα οποία ταξινομούνται σε δείγματα εισβολής 2.046 (12.5%) καθώς και δείγματα μη εισβολής: 14.272 (87.5%). Τα είδη των εισβολών είναι τύπου Spoofing και Data injection.

Το σύνολο δεδομένων αυτό έχει 44 χαρακτηριστικά τα οποία αντιστοιχούν σε 35 σχετικά με δίκτυο (Dir, Flgs, SrcAddr, DstAddr, Sport, Dport, SrcBytes, DstBytes, SrcLoad, DstLoad, SrcGap, DstGap, SIntPkt, DIntPkt, SIntPktAct, DIntPktAct, SrcJitter, DstJitter, sMaxPktSz, dMaxPktSz, sMinPktSz, dMinPktSz, Dur, Trans, TotPkts, TotBytes, Load, Loss, pLoss, pSrcLoss, pDstLoss, Rate, SrcMac, DstMac, Packet_num), 8 σχετικά με βιομετρικά δεδομένα ασθενών (Temp, SpO2, Pulse_Rate, SYS, DIA, Heart_rate, Resp_Rate, ST) και 1 χαρακτηριστικό για την ταξινόμηση (Label).

2.3.3 IoT dataset for Intrusion Detection Systems

Το σύνολο δεδομένων BoTNeTIoT-L01 [44][45][46] είναι ενσωματωμένο με το σύνολο BoTNeTIoT. Ως καινούρια έκδοση αυτού, πρακτικά έχει μειωμένες περιττές εγγραφές του αρχικού συνόλου χρησιμοποιώντας χαρακτηριστικά που αντιστοιχούν μόνο σε χρονικό παράθυρο 10 δευτερολέπτων. Περιέχει κίνηση από 9 IoT συσκευές, η οποία καταγράφηκε με χρήση του Wireshark σε τοπικό δίκτυο με χρήση κεντρικού switch: Περιέχει δύο Botnet επιθέσεις.

Συγκεκριμένα το αρχείο BoTNeTIoT-L01-v2.csv αντιστοιχεί σε 1.68 Gb δεδομένα, τα οποία είναι με label και αφορούν 1.048.575 εγγραφές. Σχετικά με τη διαθεσιμότητα του συνόλου δεδομένων, απαιτείται μόνο εγγραφή χρήστη ώστε να είναι δυνατή η μεταφόρτωση του αρχείου. Πρόκειται για εγγραφές, στις οποίες εμπεριέχονται ορισμένες όμοιες/duplicates, και αφορούν 27 χαρακτηριστικά τα οποία είναι τα MI_dir_L0.1_weight, MI_dir_L0.1_mean, MI_dir_L0.1_variance, H_L0.1_weight, H_L0.1_mean, H_L0.1_variance, HH_L0.1_weight, HH_L0.1_mean, HH_L0.1_std, HH_L0.1_magnitude, HH_L0.1_radius, HH_L0.1_covariance, HH_L0.1_pcc, HH_jit_L0.1_weight, HH_jit_L0.1_mean, HH_jit_L0.1_variance, HpHp_L0.1_weight, HpHp_L0.1_mean, HpHp_L0.1_std,

HpHp_L0.1_magnitude, HpHp_L0.1_radius, HpHp_L0.1_covariance, HpHp_L0.1_pcc, Device_Name, Attack, Attack_subType, label.

Σχετικά με την ταξινόμηση που αφορά την επίθεση, τα είδη των επιθέσεων είναι τα DDoS, DoS, OS, Service Scan, Keylogging και Data exfiltration.

2.3.4 LITNET-2020

Το σύνολο δεδομένων LITNET-2020 [32][49] έχει πραγματικά παραδείγματα εισβολών σχετικά με επιθέσεις δικτύου. Αναλύονται και περιγράφονται 84 χαρακτηριστικά και 12 διαφορετικοί τύποι επιθέσεων. Το σύνολο δεδομένων αυτό είναι δημόσιο για ερευνητικό σκοπό, και μπορεί αποτελεσματικά να αναγνωρίσει διαφορετικές επιθέσεις χρησιμοποιώντας ταξινόμηση. Τα χαρακτηριστικά αυτά απεικονίζονται στον παρακάτω πίνακα [28]:

Attribute Number	Features	Description
1	ts	Flow start time
..	..	*49 attributes that are specified*
..	..	*in NetFlow v9 [30]*
..	..	*+15 extended attributes*
64	tr	Flow received time-stamp
65	icmp-smf	Flooding network broadcast
66	icmp-f	Flooding target with ICMP packets
67	udp-f	Ddos'ing with UDP traffic
68	tcp-f-s	Flooding attack with SYN packets
69	tcp-f-n-a	Flooding attack with SYN packets
70	tcp-f-n-f	Flooding attack with SYN packets
71	tcp-f-n-r	Flooding attack with SYN packets
72	tcp-f-n-p	Flooding attack with SYN packets
73	tcp-f-n-u	Flooding attack with SYN packets
74	tcp-dst-p	Ddos'ing with HTTP traffic
75	tcp-land	Landing type of attack
76	tcp-src-tftp	Flooding TFTPservice
77	tcp-src-kerb	Flow of destination bytes
78	tcp-src-rpc	Flooding Kerberos service
79	tcp-dst-p-src	Flooding RPCservice
80	smtp-dst	Uses a vulnerability in an HTTP server
81	udp-p-r-range	Flooding with SMTP connections
82	p-range-dst	Scans on UDP ports 80, 8080, 81, etc.
83	udp-src-p-0	Several ports, one address
84	Label	Attack label

Πίνακας 6: Τα χαρακτηριστικά του συνόλου δεδομένων LITNET-2020.

Το προτεινόμενο σύνολο δεδομένων αφορά χρονική περίοδο 10 μηνών, και αφορά επιθέσεις σε 4 γεωγραφικά διακριτές περιοχές (πόλεις). Έχει σχετικά μεγάλο μέγεθος (για παράδειγμα, το csv αρχείο LITNET-2020 BLASTER_WORM_FLOWS έχει μέγεθος 1.97 Gb, labeled δεδομένων από 1.048.576 εγγραφές για τα 85 χαρακτηριστικά που αφορούν flow δικτύου με ποσοστά 88.24% μη επίθεση και 11.76% επίθεση για 12 είδη εισβολών: Smurf (0.13%), ICMP-Flood (0.03%), UDP-Flood (0.21%), TCP SYN-flood (8.22%), HTTP flood (0.05%), LAND Attack (0.12%), Blaster Worm (0.05%), Code Red Worm (2.77%), Spam Bot Detection (0.002%), Reaper Worm (0.003%), Scanning/Spread (0.01%), Packet Fragmentation Attack (0.001%)).

2.3.5 Intrusion Detection Evaluation Dataset (CIC-IDS2017)

Πρόκειται για δεδομένα με label [22][50], που αφορούν κίνηση δικτύου μοιρασμένη σε 8 αρχεία - σύνολα δεδομένων. Τα σύνολα αυτά αφορούν ώρες εργασίας για διάφορες ημέρες, όπως δείχνουν και τα ονόματα των αρχείων των συνόλων δεδομένων παρακάτω:

- Friday-WorkingHours-Afternoon-DDos.pcap_ISCX
- Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX
- Friday-WorkingHours-Morning.pcap_ISCX
- Monday-WorkingHours.pcap_ISCX
- Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX
- Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX
- Tuesday-WorkingHours.pcap_ISCX
- Wednesday-workingHours.pcap_ISCX

Το CICIDS2017 σύνολο δεδομένων περιέχει τους περισσότερο κοινούς τύπους επιθέσεων. Περιέχει επίσης τα αποτελέσματα ανάλυσης network κίνησης χρησιμοποιώντας CICFlowMeter με ροές που βασίζονται σε χαρακτηριστικά όπως ο χρόνος, source και destination IPs, source και destination ports καθώς και πρωτόκολλα. Το σύνολο δεδομένων αυτό αντιστοιχεί σε ρεαλιστική κίνηση δικτύου που δημιουργήθηκε με κύριο σκοπό να προβάλει τη συμπεριφορά ανθρώπινων αλληλεπιδράσεων. Πρόκειται για συμπεριφορά 25

χρηστών βασισμένη στα πρωτόκολλα HTTP, HTTPS, FTP, SSH, και email και σημείο αναφοράς τα κριτήρια παρακάτω:

- Complete Network configuration: Μία πλήρης δικτυακή τοπολογία που εμπεριέχει Modem, Firewall, Switches, Routers, και την παρουσία λειτουργικών συστημάτων όπως Windows, Ubuntu και Mac OS X.
- Complete Traffic: Αντιστοιχεί σε user profiling agent και 12 διαφορετικών μηχανών σε Victim-Network και πραγματικές επιθέσεις δικτύου.
- Labelled Dataset: Αντιστοιχεί σε μη εισβολή καθώς και επιθέσεις για κάθε ημέρα.
- Complete Interaction: Έχοντας δύο διαφορετικά δίκτυα, καλύπτονται οι επικοινωνίες "εντός" δικτύου και "εντός εσωτερικού LAN".
- Complete Capture: Καθώς χρησιμοποιήθηκε mirror port, π.χ. tapping system, όλες οι κινήσεις καταγράφηκαν στον server.
- Available Protocols: Αφορά την παρουσία όλων των κοινών διαθέσιμων πρωτοκόλλων, όπως HTTP, HTTPS, FTP, SSH και email.
- Attack Diversity: Περιέχει τις πιο κοινές επιθέσεις βασισμένες στο 2016 McAfee report, όπως Web based, Brute force, DoS, DDoS, Infiltration, Heart-bleed, Bot και Scan.
- Heterogeneity: Από το κύριο switch, το memory dump και απο κλήσεις του συστήματος όλων των συστημάτων που υπέστησαν εισβολή, κατά τη διάρκεια εκτέλεσης επιθέσεων, έχει καταγραφεί η κίνηση δικτύου.
- Feature Set: Πρόκειται για πάνω από 80 χαρακτηριστικά δικτύου δημιουργημένα χρησιμοποιώντας το CICFlowMeter σε csv μορφή αρχείου.
- MetaData: Επεξήγηση του συνόλου δεδομένων όπου συμπεριλαμβάνονται μονάδες όπως χρόνος και ροές.

Για παράδειγμα, το csv αρχείο με όνομα Tuesday-WorkingHours.pcap_ISCX.csv για περαιτέρω ανάλυση, επεξεργασία και αξιολόγηση, έχει μέγεθος 1.12Gb, με δεδομένα που έχουν label, που αντιστούν σε πάνω από 80 χαρακτηριστικά σχετικά με δίκτυο. Οι εγγραφές έγιναν με χρήση του CICFlowMeter και οι περιπτώσεις των επιθέσεων είναι οι Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet και DDoS. Τα χαρακτηριστικά αυτά είναι τα Flow ID, Source IP, Source Port, Destination IP, Destination Port, Protocol, Timestamp, Flow Duration, Total Fwd Packets, Total Backward Packets, Total

Length of Fwd Packets, Total Length of Bwd Packets, Fwd Packet Length Max, Fwd Packet Length Min, Fwd Packet Length Mean, Fwd Packet Length Std, Bwd Packet Length Max, Bwd Packet Length Min, Bwd Packet Length Mean, Bwd Packet Length Std, Flow Bytes/s, Flow Packets/s, Flow IAT Mean, Flow IAT Std, Flow IAT Max, Flow IAT Min, Fwd IAT Total, Fwd IAT Mean, Fwd IAT Std, Fwd IAT Max, Fwd IAT Min, Bwd IAT Total, Bwd IAT Mean, Bwd IAT Std, Bwd IAT Max, Bwd IAT Min, Fwd PSH Flags, Bwd PSH Flags, Fwd URG Flags, Bwd URG Flags, Fwd Header Length, Bwd Header Length, Fwd Packets/s, Bwd Packets/s, Min Packet Length, Max Packet Length, Packet Length Mean, Packet Length Std, Packet Length Variance, FIN Flag Count, SYN Flag Count, RST Flag Count, PSH Flag Count, ACK Flag Count, URG Flag Count, CWE Flag Count, ECE Flag Count, Down/Up Ratio, Average Packet Size, Avg Fwd Segment Size, Avg Bwd Segment Size, Fwd Header Length, Fwd Avg Bytes/Bulk, Fwd Avg Packets/Bulk, Fwd Avg Bulk Rate, Bwd Avg Bytes/Bulk, Bwd Avg Packets/Bulk, Bwd Avg Bulk Rate, Subflow Fwd Packets, Subflow Fwd Bytes, Subflow Bwd Packets, Subflow Bwd Bytes, Init_Win_bytes_forward, Init_Win_bytes_backward, act_data_pkt_fwd, min_seg_size_forward, Active Mean, Active Std, Active Max, Active Min, Idle Mean, Idle Std, Idle Max, Idle Min, Label.

2.3.6 Iot Device Network Logs (Dataset for network based IDS)

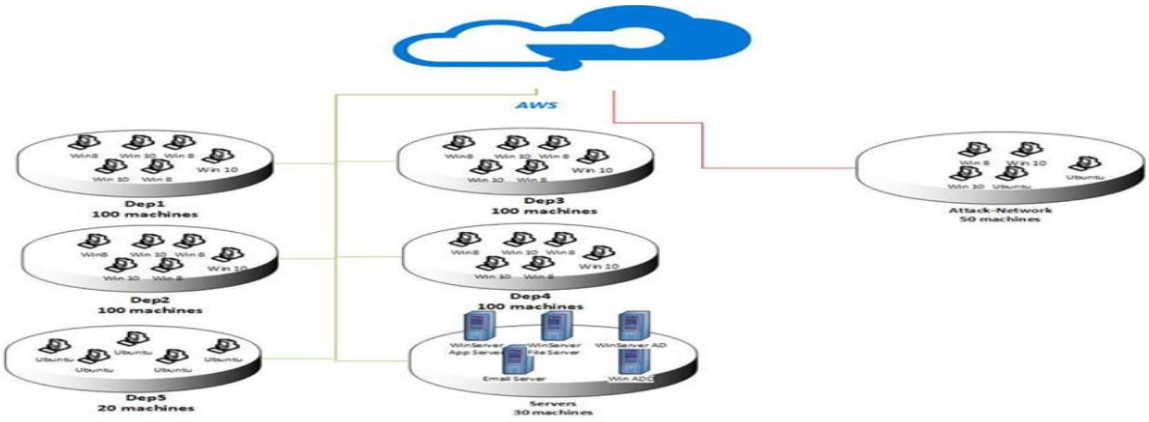
Πρόκειται για επεξεργασμένα δεδομένα σχετικά με εισβολές σε δίκτυα, με χρήση Iot συσκευές [35] Χρησιμοποιήθηκαν Ultrasonic αισθητήρες με Arduino και NodeMCU για την παρακολούθηση του δικτύου και τη συλλογή των δεδομένων. Χρησιμοποιήθηκε NodeMCU με ESP8266 wifi module για την αποστολή δεδομένων στον server μέσω wifi.

Υπάρχουν τα είδη εισβολών (χαρακτηριστικό “Value”) με τις αντιστοιχίες 0- normal, 1- wrong setup, 2- ddos, 3- Data type probing, 4 - scan attack, 5 - man in the middle. Σχετικά με το μέγεθος των αρχείων, πρόκειται για μικρά csv (για παράδειγμα το αρχείο Preprocessed_data.csv αντιστοιχεί σε 49.7 Mb, 477.427 εγγραφές (συμπεριλαμβανομένου του Label για την ταξινόμηση). Υπάρχουν 14 χαρακτηριστικά τα οποία είναι 3 σχετικά με frame (frame.number, frame.time, frame.len), 2 σχετικά με eth (eth.src, eth.dst), 4 σχετικά με ip (ip.src, ip.dst, ip.proto, ip.len), και 3 σχετικά με tcp (tcp.len, tcp.srcport, tcp.dstport), και 1 για το label ταξινόμησης (Value).

2.3.7 CSE-CIC-IDS2018

Στο σύνολο δεδομένων CSE-CIC-IDS2018 [50][58][52], δημιουργούνται επιμέρους σύνολα δεδομένων υπό την συστημική οπτική, εμπεριέχοντας έτσι λεπτομερείς περιγραφές των εισβολών καθώς και αφηρημένα μοντέλα κατανομής για εφαρμογές, πρωτόκολλα ή οντότητες χαμηλού δικτυακού επιπέδου. Τα προφίλ αυτά μπορούν να χρησιμοποιηθούν από agents ή και ανθρώπινους operators με σκοπό τη δημιουργία γεγονότων (events) σχετικά με το δίκτυο. Λόγω της αφηρημένης/ασαφούς αυτής φύσης των προφίλ αυτών, είναι δυνατή η εφαρμογή τους σε ευρύ φάσμα δικτυακών πρωτοκόλλων με ποικίλες τοπολογίες. Τα προφίλ μπορούν και να χρησιμοποιηθούν συνδυαστικά με σκοπό να δημιουργηθούν σύνολα δεδομένων για συγκεκριμένες ανάγκες.

Τα προφίλ που έχουν χτιστεί πρακτικά μπορούν να χωριστούν σε δύο διακριτές κατηγορίες προφίλ: B-profiles: Ενθυλακώνονται οι συμπεριφορές των οντοτήτων των χρηστών χρησιμοποιώντας διάφορες τεχνικές μηχανικής εκμάθησης (όπως K-Means, Random Forest, SVM, και J48). Τα αντίστοιχα χαρακτηριστικά είναι κατανομές από μεγέθη πακέτων πρωτοκόλλων, ο αριθμός πακέτων ανά ροή, ορισμένα πρότυπα στο payload, το μέγεθος του payload, καθώς και το request time του πρωτοκόλλου. Τα παρακάτω πρωτόκολλα αντιστοιχούν σε HTTPS, HTTP, SMTP, POP3, IMAP, SSH, and FTP. Τα κυριότερα όμως που έχουν χρησιμοποιηθεί είναι τα HTTP και HTTPS. M-Profiles: Αντιστοιχούν σε προσπάθειες περιγραφής επιθέσεων με ξεκάθαρο τρόπο. Η ερμηνεία των πακέτων μπορεί να γίνει από ανθρώπους και από αυτόνομους agents που κάνουν compile και εν τέλει εκτελούν τα αντίστοιχα σενάρια. Στην επόμενη εικόνα απεικονίζεται η αντίστοιχη τοπολογία δικτύου:

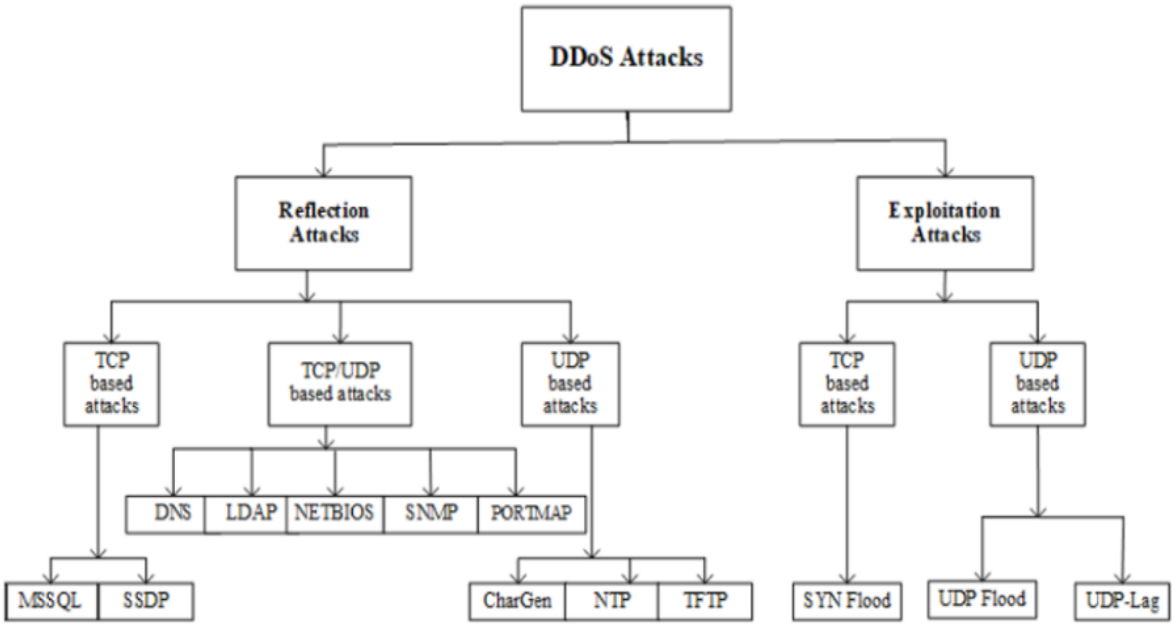


Εικόνα 11: Τοπολογία δικτύου σχετικά με την αρχιτεκτονική του CSE-CIC-IDS2018.

Το σύνολο δεδομένων αυτό έχει επιλεχθεί καθώς οι εγγραφές που του αντιστοιχούν είναι σχετικές με επιθέσεις Brute Force, DoS, Web attack, Infiltration, Botnet και PortScan.

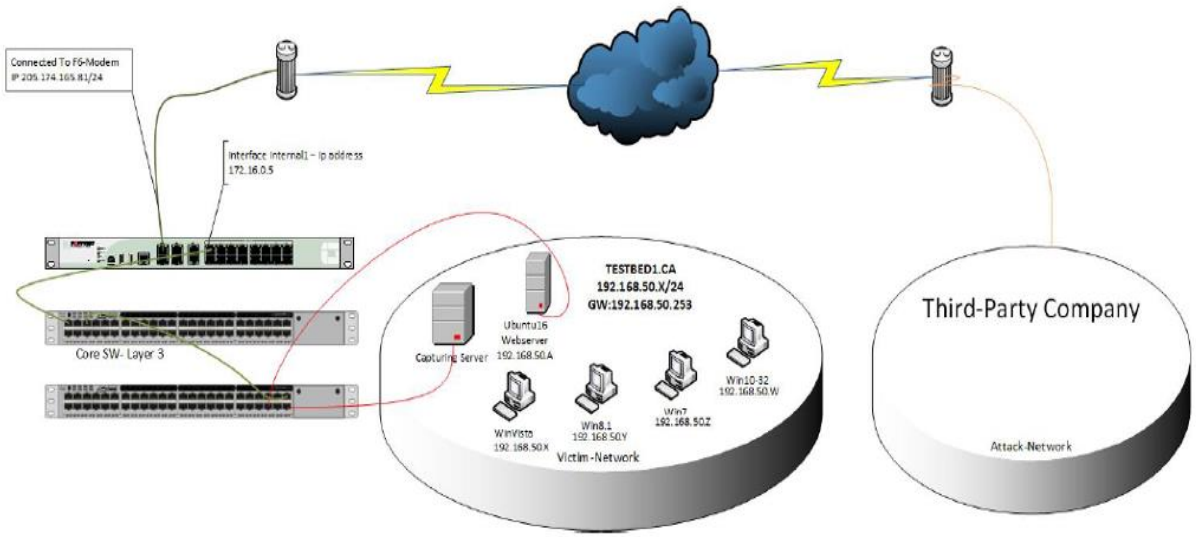
2.3.8 CIC DDoS 2019

Το σύνολο δεδομένων CIC DDoS 2019 [56][57] αντιστοιχεί σε DDoS επιθέσεις (Reflection-based DDoS και Exploitation-based) όπως απεικονίζει η παρακάτω εικόνα:



Εικόνα 12: CIC DDoS 2019 επιθέσεις.

Το σύνολο δεδομένων CIC DDoS 2019 περιέχει εγγραφές “benign” καθώς και τις πιο συνήθεις επιθέσεις τύπου DDoS. Περιέχει τα αποτελέσματα ανάλυσης κίνησης δικτύου με χρήση του CICFlowMeter-V3, βασισμένα σε μονάδες όπως ο χρόνος, οι source και destination IPs, source και destination ports καθώς και πρωτόκολλα.



Εικόνα 13: CIC DDoS 2019 testbed αρχιτεκτονική.

2.3.9 Συγκριτικός πίνακας συνόλων δεδομένων ανίχνευσης εισβολών:

Λίστα συνόλων δεδομένων						
#	**Dataset name**	**Records number**	**Features number**	**Features Category**	**Size**	**Format**
1	NSL-KDD	22544	64	Network, Host	6.3 Mb	csv
2	WUSTL EHMS 2020	16.318	44	Network, Biometric	4.4 Mb	csv
3	BoTNeTIoT-L01-v2	1.048.575	34	Network	1.68 Gb	csv
4	LITNET-2020	1.048.576	85	Network	1.97 Gb	csv
5	CIC-IDS2017 ftp and ssh attacks in file named Tuesday-WorkingHours.pcap_ISCX	445.910	80	Network	166 MB	csv

6	CIC-IDS2017 infiltration attacks in file named Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX	288.602	80	Network	103 MB	csv
7	Iot Device Network Logs	477.427	14	Network	49.7 Mb	csv
8	CSE-CIC-IDS2018 brute force attacks in file named Wednesday-14-02-2018_TrafficForML_CICFlowMeter.csv	671.139	79	Network	265 MB	csv
9	CSE-CIC-IDS2018 infiltration attacks in file named Wednesday-28-02-2018_TrafficForML_CICFlowMeter.csv	521.144	79	Network	158 MB	csv
10	CIC DDoS 2019	201079	88	Network	89.2 MB	csv

Πίνακας 7: Συγκριτικός πίνακας συνόλων δεδομένων ανίχνευσης εισβολών

Κεφάλαιο 3: Μεθοδολογία και αλγόριθμοι μηχανικής μάθησης

Στο κεφάλαιο αυτό αναφέρεται η μεθοδολογία που έχει ακολουθηθεί καθώς και οι αλγόριθμοι που χρησιμοποιήθηκαν. Πρόκειται να εξεταστεί η συμπεριφορά μοντέλων μηχανικής μάθησης που εκπαιδεύονται με ένα υποσύνολο των δεδομένων του εκάστοτε dataset, με σκοπό να γίνει αρχικά η πρόβλεψη της κλάσης (εισβολή - μη εισβολή) των υπολοίπων δειγμάτων στο ίδιο σύνολο δεδομένων, καθώς και η πρόβλεψη της κλάσης δειγμάτων από κάποιο άλλο σύνολο δεδομένων.

3.1 Μεθοδολογία

Έχει γίνει εστίαση στα σύνολα δεδομένων CIC-IDS2017 και CIC-IDS-2018. Κύριος λόγος αποτελεί το ότι τα σύνολα αυτά αναπτύχθηκαν από τον ίδιο οργανισμό, και έχουν αρκετά κοινά χαρακτηριστικά. Από το σύνολο δεδομένων CIC-IDS2017 [22][50], επιλέχθηκε το αρχείο “Tuesday-WorkingHours .pcap_ISCX.csv”, το οποίο αντιστοιχεί σε δικτυακά δεδομένα 166 MB, 445910 εγγραφών, με επικεφαλίδες 85 χαρακτηριστικών που αφορούν FTP καθώς και SSH επιθέσεις. Επίσης επιλέγεται το αρχείο “Thursday-WorkingHours-Afternoon-Infilteration .pcap_ISCX.csv”, το οποίο αντιστοιχεί σε “infiltration” επιθέσεις, έχοντας δικτυακά δεδομένα 103 MB, 288.602 εγγραφών, με τους ίδιους headers με το πρώτο. Το χαρακτηριστικό της εισβολής - ή μη εισβολής - αναφέρεται ως “Label” και έχει τις δυνατές τιμές “BENIGN”, “FTP-Patator” και “SSH-Patator” στο πρώτο αρχείο, ενώ έχει τις τιμές “BENIGN” και “Infiltration” για το δεύτερο. Η εισβολή τύπου “FTP-Patator” αποτελεί υποσύνολο των επιθέσεων ωμής βίας (brute force attacks) που αφορά το πρωτόκολλο FTP (File Transfer Protocol), συσχετίζεται δηλαδή με τη μεταφορά αρχείων. Αντίστοιχα, η εισβολή “SSH-Patator” αντιστοιχεί στο πρωτόκολλο SSH (Secure Shell Protocol), στην επικοινωνία συστημάτων δηλαδή μέσω κρυπτογραφημένων δεδομένων. Βασικός λόγος επιλογής των παραπάνω αρχείων είναι η χρήση του για εκπαίδευση και δοκιμασία μοντέλου με τα προαναφερόμενα είδη εισβολής FTP/SSH.

Η αντιστοιχία των δύο παραπάνω αρχείων με τα ψευδώνυμα τους για λόγους συντομογραφίας, είναι η εξής:

Tuesday-WorkingHours.pcap_ISCX.csv	cic_ids_2017_ftp_and_ssh_patators
Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.csv	cic_ids_2017_infiltration

Πίνακας 8: Αντιστοιχία συνόλων δεδομένων και αντίστοιχων συντομογραφιών σχετικά με το σύνολο cic_ids_2017.

Από το σύνολο δεδομένων CIC-IDS-2018 [50][58][52] χρησιμοποιείται το αρχείο με όνομα "Wednesday-28-02-2018_TrafficForML_CICFlowMeter.csv", το οποίο αντιστοιχεί σε επιθέσεις τύπου infiltration. Πρόκειται για αρχείο μεγέθους 183 MB, με 521444 εγγραφές και 79 χαρακτηριστικά. Τα δεδομένα έχουν label, σχετίζονται με παραμέτρους δικτύου και η αντίστοιχη ταξινόμηση σε εισβολή - μη εισβολή αφορά τις τιμές του χαρακτηριστικού "Label", οι οποίες είναι "Benign" και "Infiltaration". Η "Benign" τιμή αντιστοιχεί σε "μη εισβολή". Η τιμή "Infiltaration" αντιστοιχεί στον τύπο εισβολής "διείσδυση" (infiltration). Η εισβολή τύπου διείσδυσης, περιλαμβάνει την κρυφή εισαγωγή στοιχείων (assets). Έρχεται σε αντίθεση με την εισβολή "διήθηση" (exfiltration), όπου περιλαμβάνει την κρυφή αφαίρεση στοιχείων. Επίσης έχει επιλεχθεί το αρχείο "Wednesday-14-02-2018_TrafficForML_CICFlowMeter.csv", το οποίο αντιστοιχεί σε επιθέσεις τύπου FTP και SSH brute force. Το αρχείο αυτό έχει μέγεθος 265 MB, 671.139 εγγραφές και 79 χαρακτηριστικά. Το χαρακτηριστικό που αντιστοιχεί στην εισβολή έχει τις τιμές "Benign", "FTP-BruteForce", "SSH-Bruteforce". Βασικός λόγος επιλογής των παραπάνω αρχείων είναι η χρήση του για εκπαίδευση και δοκιμασία μοντέλου με τα προαναφερόμενα είδη εισβολής FTP/SSH και Infiltration. Η αντιστοιχία των δύο παραπάνω αρχείων με τα ψευδώνυμα τους για λόγους συντομογραφίας, είναι η εξής:

Wednesday-28-02-2018_TrafficForML_CICFlowMeter.csv	cic_ids_2018_infiltration
Wednesday-14-02-2018_TrafficForML_CICFlowMeter.csv	cic_ids_2018_ftp_and_ssh_brute_force

Πίνακας 9: Αντιστοιχία συνόλων δεδομένων και αντίστοιχων συντομογραφιών σχετικά με το σύνολο cic_ids_2018.

Στη συνέχεια απεικονίζονται σε πίνακα η σύνοψη των αρχείων - υποσυνόλων για περαιτέρω ανάλυση, επεξεργασία και αξιολόγηση στο πλαίσιο της διπλωματικής αυτής εργασίας.

Dataset (alias)	**cic_ids_2018_infiltration**	**cic_ids_2018_ftp_and_ssh_brute_force**	**cic_ids_2017_ftp_and_ssh_patators**	**cic_ids_2017_infiltration**
File name (with file type format)	Wednesday-28-02-2018_TrafficForML_CICFlowMeter.csv	Wednesday-14-02-2018_TrafficForML_CICFlowMeter.csv	Tuesday-WorkingHours.pcap_ISCX.csv	Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.csv
Size (uncompressed)	183 MB	265 MB	166 MB	103 MB
Rows (Headers included)	521444	671.139	445.910	288.602
Features (Intrusion classification column included)	79	79	85	85
Intrusion classification column name	Label	Label	Label	Label
Intrusion classification column values	Benign Infiltaration	Benign FTP-BruteForce SSH-Bruteforce	BENIGN FTP-Patator SSH-Patator	BENIGN Infiltration
Χαρακτηριστικά (ταξινομημένα αλφαβητικά)				
	ACK Flag Cnt	ACK Flag Cnt	ACK Flag Count	ACK Flag Count
	Active Max	Active Max	Active Max	Active Max
	Active Mean	Active Mean	Active Mean	Active Mean
	Active Min	Active Min	Active Min	Active Min
	Active Std	Active Std	Active Std	Active Std
	Pkt Size Avg	Pkt Size Avg	Average Packet Size	Average Packet Size
	Bwd Seg Size Avg	Bwd Seg Size Avg	Avg Bwd Segment Size	Avg Bwd Segment Size
	Fwd Seg Size Avg	Fwd Seg Size Avg	Avg Fwd Segment Size	Avg Fwd Segment Size
	Bwd Blk Rate Avg	Bwd Blk Rate Avg	Bwd Avg Bulk Rate	Bwd Avg Bulk Rate

	Bwd Byts/b Avg	Bwd Byts/b Avg	Bwd Avg Bytes/Bulk	Bwd Avg Bytes/Bulk
	Bwd Pkts/b Avg	Bwd Pkts/b Avg	Bwd Avg Packets/Bulk	Bwd Avg Packets/Bulk
	Fwd Seg Size Min	Fwd Seg Size Min	min_seg_size_forward	min_seg_size_forward
	Fwd Pkts/b Avg	Fwd Pkts/b Avg	Fwd Avg Packets/Bulk	Fwd Avg Packets/Bulk
	Bwd Header Len	Bwd Header Len	Bwd Header Length	Bwd Header Length
	Bwd IAT Max	Bwd IAT Max	Bwd IAT Max	Bwd IAT Max
	Bwd IAT Mean	Bwd IAT Mean	Bwd IAT Mean	Bwd IAT Mean
	Bwd IAT Min	Bwd IAT Min	Bwd IAT Min	Bwd IAT Min
	Bwd IAT Std	Bwd IAT Std	Bwd IAT Std	Bwd IAT Std
	Bwd IAT Tot	Bwd IAT Tot	Bwd IAT Total	Bwd IAT Total
	Bwd PSH Flags	Bwd PSH Flags	Bwd PSH Flags	Bwd PSH Flags
	Bwd Pkt Len Max	Bwd Pkt Len Max	Bwd Packet Length Max	Bwd Packet Length Max
	Bwd Pkt Len Mean	Bwd Pkt Len Mean	Bwd Packet Length Mean	Bwd Packet Length Mean
	Bwd Pkt Len Min	Bwd Pkt Len Min	Bwd Packet Length Min	Bwd Packet Length Min
	Bwd Pkt Len Std	Bwd Pkt Len Std	Bwd Packet Length Std	Bwd Packet Length Std
	Bwd Pkts/s	Bwd Pkts/s	Bwd Packets/s	Bwd Packets/s
	Bwd URG Flags	Bwd URG Flags	Bwd URG Flags	Bwd URG Flags
	CWE Flag Count	CWE Flag Count	CWE Flag Count	CWE Flag Count
			Destination IP	Destination IP
	Dst Port	Dst Port	Destination Port	Destination Port
	Down/Up Ratio	Down/Up Ratio	Down/Up Ratio	Down/Up Ratio
	ECE Flag Cnt	ECE Flag Cnt	ECE Flag Count	ECE Flag Count
	FIN Flag Cnt	FIN Flag Cnt	FIN Flag Count	FIN Flag Count
	Flow Byts/s	Flow Byts/s	Flow Bytes/s	Flow Bytes/s
	Flow Duration	Flow Duration	Flow Duration	Flow Duration

	Flow IAT Max	Flow IAT Max	Flow IAT Max	Flow IAT Max
	Flow IAT Mean	Flow IAT Mean	Flow IAT Mean	Flow IAT Mean
	Flow IAT Min	Flow IAT Min	Flow IAT Min	Flow IAT Min
	Flow IAT Std	Flow IAT Std	Flow IAT Std	Flow IAT Std
			Flow ID	Flow ID
	Flow Pkts/s	Flow Pkts/s	Flow Packets/s	Flow Packets/s
	Fwd Blk Rate Avg	Fwd Blk Rate Avg	Fwd Avg Bulk Rate	Fwd Avg Bulk Rate
	Fwd Act Data Pkts	Fwd Act Data Pkts	act_data_pkt_fwd	act_data_pkt_fwd
	Fwd Byts/b Avg	Fwd Byts/b Avg	Fwd Avg Bytes/Bulk	Fwd Avg Bytes/Bulk
	Fwd Header Len	Fwd Header Len	Fwd Header Length	Fwd Header Length
			~~Fwd Header Length~~	~~Fwd Header Length~~
	Fwd IAT Max	Fwd IAT Max	Fwd IAT Max	Fwd IAT Max
	Fwd IAT Mean	Fwd IAT Mean	Fwd IAT Mean	Fwd IAT Mean
	Fwd IAT Min	Fwd IAT Min	Fwd IAT Min	Fwd IAT Min
	Fwd PSH Flags	Fwd PSH Flags	Fwd PSH Flags	Fwd PSH Flags
	Fwd IAT Std	Fwd IAT Std	Fwd IAT Std	Fwd IAT Std
	Fwd IAT Tot	Fwd IAT Tot	Fwd IAT Total	Fwd IAT Total
	Fwd Pkt Len Max	Fwd Pkt Len Max	Fwd Packet Length Max	Fwd Packet Length Max
	Fwd Pkt Len Mean	Fwd Pkt Len Mean	Fwd Packet Length Mean	Fwd Packet Length Mean
	Fwd Pkt Len Min	Fwd Pkt Len Min	Fwd Packet Length Min	Fwd Packet Length Min
	Fwd Pkt Len Std	Fwd Pkt Len Std	Fwd Packet Length Std	Fwd Packet Length Std
	Fwd Pkts/s	Fwd Pkts/s	Fwd Packets/s	Fwd Packets/s
	Fwd URG Flags	Fwd URG Flags	Fwd URG Flags	Fwd URG Flags
	Idle Max	Idle Max	Idle Max	Idle Max
	Idle Mean	Idle Mean	Idle Mean	Idle Mean

	Idle Min	Idle Min	Idle Min	Idle Min
	Idle Std	Idle Std	Idle Std	Idle Std
	Init Bwd Win Byts	Init Bwd Win Byts	Init_Win_bytes_backward	Init_Win_bytes_backward
	Init Fwd Win Byts	Init Fwd Win Byts	Init_Win_bytes_forward	Init_Win_bytes_forward
	Label	Label	Label	Label
	Pkt Len Max	Pkt Len Max	Max Packet Length	Max Packet Length
	Pkt Len Min	Pkt Len Min	Min Packet Length	Min Packet Length
	PSH Flag Cnt	PSH Flag Cnt	PSH Flag Count	PSH Flag Count
	Pkt Len Mean	Pkt Len Mean	Packet Length Mean	Packet Length Mean
	Pkt Len Std	Pkt Len Std	Packet Length Std	Packet Length Std
	Pkt Len Var	Pkt Len Var	Packet Length Variance	Packet Length Variance
	Protocol	Protocol	Protocol	Protocol
	RST Flag Cnt	RST Flag Cnt	RST Flag Count	RST Flag Count
	SYN Flag Cnt	SYN Flag Cnt	SYN Flag Count	SYN Flag Count
			Source IP	Source IP
			Source Port	Source Port
	Subflow Bwd Byts	Subflow Bwd Byts	Subflow Bwd Bytes	Subflow Bwd Bytes
	Subflow Bwd Pkts	Subflow Bwd Pkts	Subflow Bwd Packets	Subflow Bwd Packets
	Subflow Fwd Byts	Subflow Fwd Byts	Subflow Fwd Bytes	Subflow Fwd Bytes
	Subflow Fwd Pkts	Subflow Fwd Pkts	Subflow Fwd Packets	Subflow Fwd Packets
			Timestamp	Timestamp
	Tot Bwd Pkts	Tot Bwd Pkts	Total Backward Packets	Total Backward Packets
	Tot Fwd Pkts	Tot Fwd Pkts	Total Fwd Packets	Total Fwd Packets

	TotLen Bwd Pkts	TotLen Bwd Pkts	Total Length of Bwd Packets	Total Length of Bwd Packets
	TotLen Fwd Pkts	TotLen Fwd Pkts	Total Length of Fwd Packets	Total Length of Fwd Packets
	URG Flag Cnt	URG Flag Cnt	URG Flag Count	URG Flag Count

Πίνακας 10: Τα επιλεγμένα προς επεξεργασία σύνολα δεδομένων με τα χαρακτηριστικά τους.

Όπως φαίνεται από τον παραπάνω πίνακα, τα ποσοστά κοινών χαρακτηριστικών μεταξύ των τριών επιλεγμένων συνόλων δεδομένων, είναι πάνω από 90%. Από σημαίνει πως είναι εφικτή η σύγκριση των δεδομένων αυτών. Κλιμάκωση μεταξύ των πεδίων στα σύνολα δεδομένων δεν απαιτείται (με εξαίρεση το πεδίο της ταξινόμησης), καθώς βρέθηκαν ίδιες μονάδες μέτρησης στα χαρακτηριστικά αυτά. Αυτό σημαίνει πως δεν χρειάζεται σχετική ομαλοποίηση καθώς έχουν την ίδια σημασία οι τιμές των πεδίων. Το χαρακτηριστικό με όνομα “Label” είναι αυτό που αντιστοιχεί στην ταξινόμηση (εισβολή - μη εισβολή). Οι επιτρεπτές τιμές του για κάθε σύνολο δεδομένων αναγράφεται στον παραπάνω πίνακα. Όπως φαίνεται, στο πεδίο αυτό χρειάζεται επεξεργασία καθώς οι επιτρεπτές τιμές δεν είναι ίδιες.

Το χαρακτηριστικό με όνομα “Fwd Header Length” αποτελεί διπλή εγγραφή (duplicate) για το σύνολο “CIC-IDS2017”. Αυτό σημαίνει πως κατά την προεπεξεργασία του συνόλου, αφαιρείται η διπλή στήλη με όνομα “Fwd Header Length”. Κατά την επεξεργασία του συνόλου “CIC-IDS-2018”, γίνεται μετατροπή των ονομάτων των επικεφαλίδων με σκοπό την λειτουργική κοινή ονομασία αυτών σε σχέση με τα άλλα δύο σύνολα (τα οποία έχουν ίδια ονόματα στηλών-χαρακτηριστικών). Έπειτα, αναφέρεται ο τρόπος χρήσης των συνόλων δεδομένων. Στη πράξη πρόκειται για βήματα που ακολουθήθηκαν, αποσκοπώντας στην πρόβλεψη κλάσης (εισβολής - μη εισβολής), στο πλαίσιο εξέτασης τριών σεναρίων:

Σενάριο	Σύνολο εκπαίδευσης μοντέλου	Σύνολο αξιολόγησης μοντέλου
A	cic_ids_2018_infiltration	cic_ids_2017_infiltration
B	cic_ids_2018_ftp_and_ssh_brute_force	cic_ids_2017_ftp_and_ssh_patators
Γ	cic_ids_2018_infiltration	cic_ids_2017_ftp_and_ssh_patators

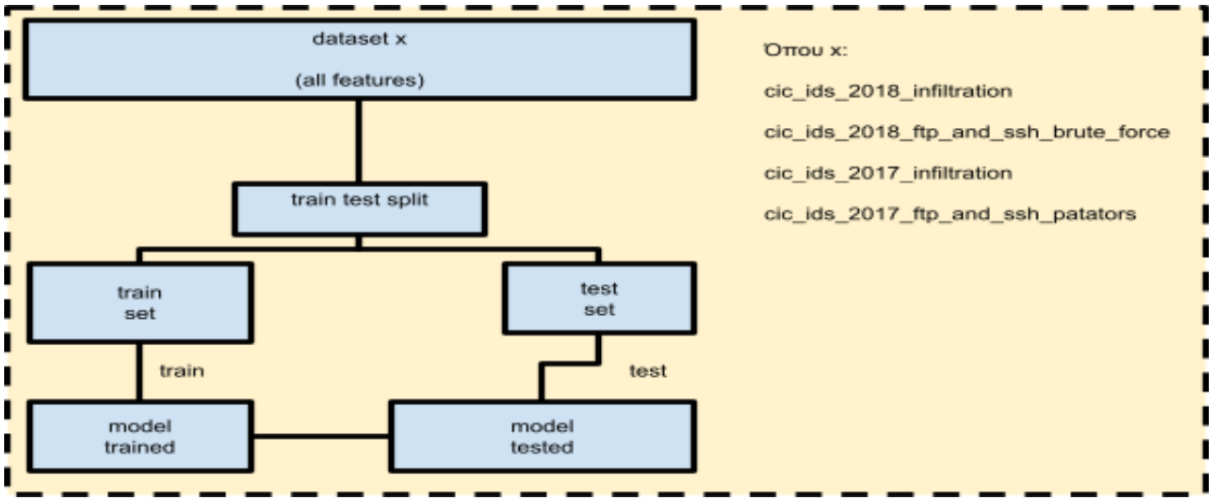
Πίνακας 11: Σενάρια υπό εξέταση στην διπλωματική εργασία.

Στο σενάριο Α, σε πρώτο βήμα α1, διαχωρίζεται το σύνολο cic_ids_2018_infiltration σε υποσύνολα εκπαίδευσης και δοκιμασίας, έτσι ώστε να εκπαιδευτεί ένα μοντέλο με βάση το πρώτο υποσύνολο και να αξιολογηθεί έπειτα από το δεύτερο υποσύνολο. Σε δεύτερο βήμα α2, γίνονται οι ίδιες ενέργειες για το σύνολο δεδομένων cic_ids_2017_infiltration. Τα βήματα αυτά α1 και α2, έχουν σκοπό να αποδείξουν πως το κάθε ένα από τα σύνολα cic_ids_2018_infiltration και cic_ids_2017_infiltration μπορούν να αξιολογήσουν μοντέλο που εκπαιδεύεται από το ίδιο εκάστοτε σύνολο, με απώτερο σκοπό τη χρήση τους στο τρίτο βήμα που αναφέρεται στη συνέχεια. Σε τρίτο βήμα α3, εκπαιδεύεται ένα μοντέλο με βάση το υποσύνολο εκπαίδευσης του cic_ids_2018_infiltration, και το μοντέλο αυτό δοκιμάζεται στο υποσύνολο δοκιμασίας του cic_ids_2017_infiltration.

Στο σενάριο Β, με την ίδια λογική που έχει ακολουθηθεί στο σενάριο Α, εφαρμόζονται δύο βήματα όπου μεμονωμένα τα σύνολα cic_ids_2018_ftp_and_ssh_brute_force (βήμα β1) και cic_ids_2017_ftp_and_ssh_patators (βήμα β2) διαχωρίζονται σε υποσύνολα εκπαίδευσης και δοκιμασίας, εκπαιδεύοντας μοντέλα που αξιολογούνται στο ίδιο εκάστοτε σύνολο. Έπεται το βήμα β3, όπου εκπαιδεύεται ένα μοντέλο με βάση το υποσύνολο εκπαίδευσης του cic_ids_2018_ftp_and_ssh_brute_force , και το μοντέλο αυτό δοκιμάζεται στο υποσύνολο δοκιμασίας του cic_ids_2017_ftp_and_ssh_patators.

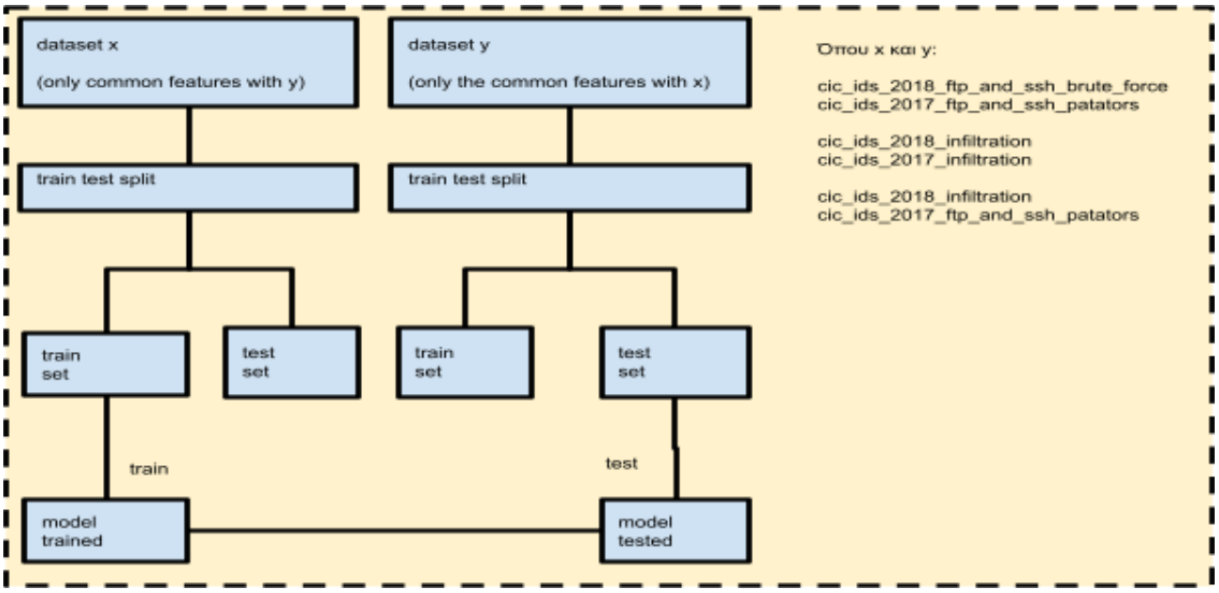
Στο σενάριο Γ, εκπαιδεύεται ένα μοντέλο με βάση το υποσύνολο εκπαίδευσης του cic_ids_2018_infiltration, και το μοντέλο αυτό δοκιμάζεται στο υποσύνολο δοκιμασίας του cic_ids_2017_ftp_and_ssh_patators (βήμα γ1). Δεν εφαρμόζονται επιπλέον βήματα εκπαίδευσης-δοκιμασίας σε κάθε ένα από τα cic_ids_2018_infiltration και cic_ids_2017_ftp_and_ssh_patators, καθώς τα βήματα αυτά έχουν ήδη υλοποιηθεί (βήματα α1 και β2 αντίστοιχα).

Για κάθε ένα από τα σενάρια που υλοποιήθηκαν, εφαρμόστηκε ξεχωριστό βήμα όπου το εκάστοτε σύνολο δεδομένο εκπαιδεύει μοντέλο, το οποίο χρησιμοποιείται για την αξιολόγηση του ίδιου συνόλου, όπως φαίνεται στη συνέχεια:



Εικόνα 14: Βήματα σεναρίων που αντιστοιχούν στην εκπαίδευση και δοκιμασία του ίδιου συνόλου.

Τα τρία σενάρια που υλοποιήθηκαν απεικονίζονται παρακάτω:



Εικόνα 15: Βήματα σεναρίων που αντιστοιχούν στην εκπαίδευση και δοκιμασία διαφορετικών συνόλων.

Με σκοπό την αξιολόγηση των αποτελεσμάτων, θα χρησιμοποιηθούν οι μετρικές (metrics) ορθότητας (accuracy), ακρίβειας (precision), ανάκλησης (pecall), F1:

Ο πίνακας σύγχυσης (confusion matrix) περιέχει το σύνολο των προβλεπόμενων και πραγματικών κλάσεων, όπου TP = True Positive (Αληθώς Θετικό), FP = False Positive (Ψευδώς Θετικό), TN = True Negative (Αληθώς Αρνητικό), FN = False Negative (Ψευδώς Αρνητικό), όπως απεικονίζονται παρακάτω:

	προβλεπόμενη τάξη (predicted class)		
πραγματική τάξη (actual class)		Class = Yes	Class = No
	Class = Yes	TP f11	FN f10
	Class = No	FP f01	TN f00

Πίνακας 12: Πίνακας σύγχυσης με το σύνολο των προβλεπόμενων και πραγματικών κλάσεων.

Η ορθότητα (accuracy) αποτελεί το συνηθέστερο μέτρο αξιολόγησης, και δίνεται από τον παρακάτω τύπο:

$$\text{Accuracy} = \frac{f_{11} + f_{00}}{f_{11} + f_{00} + f_{01} + f_{10}} = \frac{TP + TN}{TP + TN + FP + FN}$$

Ο αντίστοιχος λόγος λάθους (error rate), όπου error rate (c) = 1 – accuracy (c), μπορεί να βρεθεί από την παρακάτω σχέση:

$$\text{Λόγος Λάθους: } \text{Error rate} = \frac{f_{01} + f_{10}}{f_{11} + f_{00} + f_{01} + f_{10}}$$

Η ανάκληση (recall) δείχνει το πόσα από τα θετικά παραδείγματα έχει καταφέρει να βρει ο ταξινομητής. Όσο αυξάνεται η ανάκληση, τόσο λιγότερα θετικά παραδείγματα έχουν ταξινομηθεί λάθος. Η ανάκληση (r) δίνεται από τον παρακάτω τύπο:

$$\text{r} = \frac{TP}{TP + FN}$$

Η ακρίβεια (precision) δείχνει πόσα από τα παραδείγματα που ταξινομήθηκαν ως θετικά, είναι όντως θετικά. όσο αυξάνεται η ακρίβεια, τόσο μειώνεται το πλήθος των ψευδώς θετικών (false positive). Η ακρίβεια (p) δίνεται από τον παρακάτω τύπο:

$$\text{p} = \frac{TP}{TP + FP}$$

Η τιμή F αντιστοιχεί στον αρμονικό μέσο (harmonic mean), ο οποίος και τείνει να είναι πλησιέστερα στο μικρότερο εκ των δύο. Στον αρμονικό μέσο, η υψηλή τιμή σημαίνει πως και τα δύο είναι επαρκώς μεγάλα. Η μετρική F1 δίνεται από τον παρακάτω τύπο:

$$F_1 = \frac{2rp}{r+p} = \frac{2TP}{2TP+FP+FN} \quad , \quad F_1 = \frac{2}{1/r+1/p}$$

3.2 Αλγόριθμοι μηχανικής μάθησης

Η επιβλεπόμενη μάθηση [73] είναι μία κατηγορία της μηχανικής μάθησης. Αποτελεί τη διεργασία κατά την οποία μία συνάρτηση μαθαίνει να αντιστοιχεί μία είσοδο σε μία έξοδο, με βάση ζεύγη εισόδων-εξόδων. Η ταξινόμηση (classification) είναι μία τεχνική κατηγοριοποίησης συνόλων δεδομένων σε κλάσεις (τάξεις) μέσω της πρόβλεψης της κατηγορίας των δεδομένων σημείων. Οι κλάσεις αυτές αναφέρονται και ως στόχος (target), ετικέτες (labels) ή και κατηγορίες (categories). Η παλινδρόμηση (regression) είναι μία κατηγορία της μηχανικής μάθησης όπου η έξοδος προσεγγίζει πραγματικές τιμές και όχι απαραίτητα δυαδικές. Είναι μία μέθοδος μοντελοποίησης τιμής στόχου η οποία βασίζεται σε ανεξάρτητους προγνωστικούς παράγοντες. Η παλινδρόμηση κυρίως χρησιμοποιείται για την πρόβλεψη και εντοπισμό της σχέσης αιτίου-αποτελέσματος μεταξύ των μεταβλητών.

Η μη επιβλεπόμενη μάθηση είναι μία κατηγορία μηχανικής μάθησης που αποσκοπεί στην ανακάλυψη πιθανής δομής δεδομένων τα οποία δεν είναι χαρακτηρισμένα. Για παράδειγμα, η συσταδοποίηση (clustering) σχετίζεται με την τμηματοποίηση (partitioning) συνόλων δεδομένων σε συστάδες ώστε τα στοιχεία του συνόλου δεδομένων που ανήκουν σε μία συστάδα να μοιάζουν περισσότερο συγκριτικά με τα στοιχεία των υπόλοιπων συστάδων.

Η ενισχυτική μάθηση (reinforcement learning) είναι μία τεχνική μηχανικής μάθησης, σύμφωνα με την οποία το σύστημα μαθαίνει αλληλεπιδρώντας με το περιβάλλον του. Βασίζεται στην επιβράβευση και τιμωρία επιθυμητών και μη επιθυμητών συμπεριφορών αντίστοιχα. Η βασική αρχή λειτουργίας αντιστοιχεί σε ενέργειες δοκιμής και λάθους (trial and error).

Στη διπλωματική αυτή εργασία, έχει γίνει εστίαση στους αλγορίθμους επιβλεπόμενης μάθησης, και συγκεκριμένα στην ταξινόμηση. Οι αλγόριθμοι που έχουν επιλεχθεί είναι οι Gaussian Naive Bayes, K Nearest Neighbors, Decision Tree, Random Forest, MLP, Logistic Regression καθώς και SVM. Σκοπός τους είναι να εφαρμοστούν στο πλαίσιο της ταξινόμησης,

σχετικά με την ανίχνευση εισβολών. Οι αλγόριθμοι αυτοί, από πλευράς προγραμματισμού, παρέχονται από τη βιβλιοθήκη sklearn [68] που χρησιμοποιήθηκε στο πλαίσιο της διπλωματικής εργασίας.

3.2.1 Gaussian Naive Bayes

Ο αλγόριθμος Gaussian Naive Bayes (GNB) πρακτικά χρησιμοποιεί τον νόμο του Bayes:

$$P(A|B) = (P(B|A)\ P(A)) \ / \ (P(B))$$

Εφαρμόζεται η naive υπόθεση θεωρώντας πως υπάρχει σύνολο δεδομένων με ανεξάρτητα χαρακτηριστικά (κάτι το οποίο δεν συνηθίζεται πάντα). Έχοντας τη μεταβλητή κλάσης y, καθώς και ένα εξαρτώμενο διάνυσμα n χαρακτηριστικών ($x1$, …, xn), σύμφωνα με το παραπάνω θεώρημα Bayes προκύπτει:

$$P(y|x1,\ldots,xn) = (P(y)P(x1,\ldots xn|y)) \ / \ (P(x1,\ldots,xn))$$

Θεωρόντας ότι $P(x1,\ldots,xi,\ldots,xn \mid y) = \prod P(xi \mid y,x1,\ldots,xi-1,xi+1,\ldots,xn)$ και ότι κάθε xi εξαρτάται μόνο από την εκάστοτε κλάση y (ανεξάρτητα features), έχουμε:

$$P(xi|y,x1,\ldots,xi-1,xi+1,\ldots,xn)=P(xi|y)$$

Με άλλα λόγια, μπορούμε να ορίσουμε την παρακάτω σχέση:

$$P(y|x1,\ldots,xn)=(P(y)\prod P(xi|y))/(P(x1,\ldots,xn))$$

Θεωρώντας $P(x1,\ldots,xn)$ σταθερό, καταλήγουμε στο ότι η P(y) υπόθεση είναι ίση με τη σχετική συχνότητα της κλάσης y στο training σύνολο, δηλαδή:

$$\hat{y} = \arg\ y\ \max P(y)\ (\prod P(xi|y))$$

Πρακτικά η $P(xi|y)$ είναι η πιθανότητα του δείγματος για τη δεδομένη υπόθεση. Η πιθανότητα αυτή υπολογίζεται από το σύνολο εκπαίδευσης (training set). Υπάρχει μία ποικιλία Naive

Bayes ταξινομητών όπου υποθέτουν διαφορετικές κατανομές. Έτσι, ο Gaussian Naive Bayes ταξινομητής υποθέτει Gaussian κατανομή $P(xi|y)$.

Σύμφωνα με τα παραπάνω, ο αλγόριθμος αυτός υποθέτει ότι τα δεδομένα είναι ανεξάρτητα μεταξύ τους και προέρχονται από μια συγκεκριμένη κατανομή (η οποία καλείται να βρεθεί). Ο Naive Bayes ταξινομητής θεωρεί επίσης πως τα χαρακτηριστικά για κάθε εγγραφή είναι ανεξάρτητα μεταξύ τους. Συγκεκριμένα, ο Gaussian Naive Bayes ταξινομητής θεωρεί πως οι τιμές των χαρακτηριστικών ακολουθούν την κανονική κατανομή.

3.2.2 KNN

Ο αλγόριθμος KNN αφορά τους k-πλησιέστερους γείτονες (k-nearest neighbors). Ο αλγόριθμος αυτός για κάθε νέο δείγμα εντοπίζει τα k πλησιέστερα δείγματα που υπάρχουν στα train/annotated δεδομένα. Το αποτέλεσμα είναι να αποκτήσει το νέο δείγμα την ετικέτα που έχουν τα περισσότερα από αυτά.

Απαιτείται σχετικά μεγάλος χρόνος υπολογισμού κατά τη διαδικασία ταξινόμησης με αυτόν τον αλγόριθμο, καθώς και υπολογιστικοί πόροι (μνήμη). Μειονέκτημα αποτελεί για τον KNN η ευαισθησία που σχετίζεται με την επιλογή του μέτρου της προαναφερόμενης απόστασης καθώς και το γεγονός ότι δεν υπάρχει αποδοτικός αυτοματοποιημένος τρόπος εύρεσης του βέλτιστου k. Συνήθως χρησιμοποιείται σε περιπτώσεις που τα σύνολα δεδομένων δεν έχουν υπερβολικά μεγάλο μέγεθος, και χρησιμοποιείται συχνά καθώς είναι απλός.

3.2.3. Decision Tree

Τα δέντρα απόφασης μπορούν να είναι δύο κατηγοριών. Η πρώτη κατηγορία αφορά τα δέντρα ταξινόμησης (classification trees): Η ανάλυση δέντρων ταξινόμησης αντιστοιχεί στην περίπτωση όπου το προσδοκώμενο αποτέλεσμα είναι διακριτή τιμή (η τάξη στην οποία ανήκουν τα δεδομένα). Η δεύτερη κατηγορία αφορά τα δέντρα παλινδρόμησης (regression trees): Η ανάλυση δέντρων παλινδρόμησης αντιστοιχεί στην περίπτωση όπου το προσδοκώμενο αποτέλεσμα μπορεί να θεωρηθεί ένας πραγματικός αριθμός (π.χ. δεκαδικός αριθμός).

Ο όρος ανάλυση δέντρου ταξινόμησης και παλινδρόμησης (classification and regression tree, CART) αναφέρεται πρακτικά στις δύο προαναφερόμενες διαδικασίας. Τα δέντρα που χρησιμοποιούνται για ταξινόμηση καθώς και τα δέντρα που χρησιμοποιούνται για παλινδρόμηση, ενώ έχουν κοινά στοιχεία, διαφοροποιούνται ορατά σε διαδικασίες όπως αυτή που καθορίζει τον διαχωρισμό (split) των δεδομένων.

Ο αλγόριθμος Decision Tree (δέντρο απόφασης) [64][65] πρακτικά δημιουργεί ένα μοντέλο - δέντρο και αντιστοιχεί στη λογική του "διαίρει και βασίλευε", διαιρώντας έτσι τον χώρο όπου γίνεται η αναζήτηση στο πλαίσιο του συνόλου δεδομένων σε ορθογώνιες υποπεριοχές - υποσύνολα με βάση τις τιμές των χαρακτηριστικών. Οι εσωτερικοί κόμβοι του δέντρου ονοματίζονται με το όνομα ενός χαρακτηριστικού, και κάθε κλαδί ονοματίζεται με κάποιο κατηγόρημα.

3.2.4 Random Forest

Ο αλγόριθμος Random Forest (τυχαίο δάσος) [66][67] είναι μία μέθοδος μηχανικής εκμάθησης για διεργασίες όπως η ταξινόμηση και η παλινδρόμηση. Πρακτικά δημιουργεί πολλά δέντρα αποφάσεων κατά τον χρόνο εκπαίδευσης. Στην περίπτωση της ταξινόμησης, το αποτέλεσμα του αλγορίθμου είναι η τάξη (κλάση) που επιλέχθηκε από τα περισσότερα δέντρα. Στην περίπτωση της παλινδρόμησης, επιστρέφεται η μέση πρόβλεψη (μέση τιμή) των μεμονωμένων δέντρων. Ένα πλεονέκτημα των Random Forest αλγορίθμων είναι το ότι δεν κάνουν overfit. Η απόδοση τους στο σύνολο δοκιμής (test performance) δεν μειώνεται λόγω του overfitting καθώς αυξάνεται ο αριθμός των δέντρων, τείνει παρόλα αυτά να παραμένει σε συγκεκριμένη τιμή.

Οι αλγόριθμοι Random Forest γενικά έχουν καλύτερη απόδοση σε σχέση με τα δέντρα απόφασης, παρόλα αυτά έχουν χαμηλότερη ακρίβεια (Accuracy) σε σχέση με τα gradient boosted trees. Επίσης, τα χαρακτηριστικά μπορούν να επηρεάσουν την απόδοσή τους.

3.2.5 MLP

Ο αλγόριθμος MLP (Multi-layer Perceptron) [60][61][62] πρακτικά έχει ένα επίπεδο εισόδου, ένα εξόδου και ένα ή περισσότερα ενδιάμεσα επίπεδα όπου συνδυάζει τα δεδομένα των κόμβων του προηγούμενου επιπέδου, και ακολούθως εφαρμόζει την συνάρτηση ενεργοποίησης (π.χ. βηματική, logistic, tan, Rectified Linear Unit (ReLU)) με σκοπό να βρει την πληροφορία που πρόκειται να μεταδώσει στους επόμενους κόμβους.

Λόγω της αρχιτεκτονικής του, ο αλγόριθμος αυτός έχει τη δυνατότητα να διαχειριστεί αποτελεσματικά σχετικά περίπλοκες περιπτώσεις κατηγοριοποίησης όπου τα δεδομένα δεν είναι γραμμικά διαχωρίσιμα.

3.2.6 Logistic Regression

Η Logistic Regression (λογιστική παλινδρόμηση) αποτελεί μία μέθοδο ταξινόμησης που χρησιμοποιεί την logistic συνάρτηση με σκοπό να μοντελοποιήσει εξαρτημένες μεταβλητές. Ο αλγόριθμος Logistic regression, προσπαθεί να βρει μια ευθεία (όταν πρόκειται για δύο διαστάσεις) ή ένα υπερεπίπεδο (όταν πρόκειται για τρεις ή περισσότερες διαστάσεις) που να διαχωρίζει τα δεδομένα σε δύο κατηγορίες.

3.2.7 SVM

Ο αλγόριθμος SVM (Support Vector Machine) προσπαθεί να βρει μια ευθεία (στην περίπτωση των δύο διαστάσεων) ή γενικότερα ένα υπερεπίπεδο (στην περίπτωση τριών ή περισσότερων διαστάσεων) που να διαχωρίζει τα δεδομένα των δύο κλάσεων, με τέτοιο τρόπο έτσι ώστε η απόστασή τους από το υπερεπίπεδο αυτό να είναι η μέγιστη δυνατή. Έτσι, ο SVM εστιάζει γενικότερα σε γραμμικά (ή κατά προσέγγιση γραμμικά) διαχωρίσιμα προβλήματα. Στην περίπτωση που δεν πρόκειται για γραμμικά, γίνεται χρήση του “τεχνάσματος πυρήνα” (kernel trick), όπου μπορεί να επιτρέψει την μετάβαση σε έναν νέο χώρο όπου τα δεδομένα μπορούν να διαχωριστούν καλύτερα.

Κεφάλαιο 4: Αποτελέσματα και σχολιασμός

4.1 Σενάρια και προεπεξεργασία δεδομένων

Στο πρώτο σενάριο που εξετάζεται, το σύνολο δεδομένων cic_ids_2018_infiltration εκπαιδεύει ένα μοντέλο και έπειτα το μοντέλο αυτό αξιολογείται από το σύνολο cic_ids_2017_infiltration. Στο δεύτερο σενάριο, εκπαιδεύεται μοντέλο με βάση το σύνολο cic_ids_2018_ftp_and_ssh_brute_force και έπειτα αξιολογείται με βάση το cic_ids_2017_ftp_and_ssh_patators σύνολο. Στο τρίτο σενάριο, εκπαιδεύεται μοντέλο με βάση το σύνολο cic_ids_2018_infiltration και έπειτα το μοντέλο αξιολογείται με βάση το σύνολο cic_ids_2017_ftp_and_ssh_patators. Τα τρία αυτά σενάρια εμπεριέχουν βήματα κατά τα οποία τα μοντέλα έχουν επιπλέον αξιολογηθεί από τα ίδια τα σύνολα που εκπαιδεύτηκαν. Τέλος, κάθε διαδικασία εκπαίδευσης και αξιολόγησης γίνεται ενώ έχει προηγηθεί διαχωρισμός του εκάστοτε συνόλου σε υποσύνολα εκπαίδευσης και αξιολόγησης ώστε αυτά να χρησιμοποιηθούν αντίστοιχα.

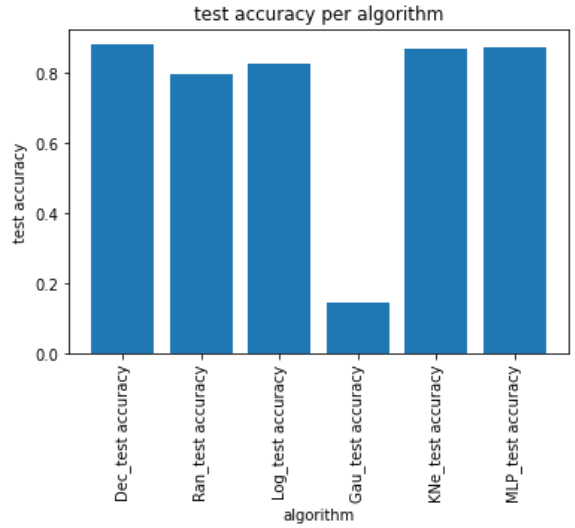
Η επεξεργασία που έγινε αφορά κυρίως εγγραφές με κενά πεδία, καθώς και με μετασχηματισμό τιμών των χαρακτηριστικών που έχουν αλφαριθμητικές τιμές/ χαρακτήρες/ σύμβολα σε τιμές αριθμητικές τιμές. Επίσης χειρίστηκε το πρόβλημα των πεδίων με τιμές που θεωρούνται “άπειρες”, διαχωρίστηκε η γραμμή των headers από τις υπόλοιπες γραμμές που αντιστοιχούν στα πραγματικά δεδομένων. Τα σύνολα δεδομένων που έχουν χρησιμοποιηθεί στη διπλωματική εργασία, από πλευράς προγραμματισμού, χωρίστηκαν σε train και test υποσύνολα με χρήση της βιβλιοθήκης sklearn [68]. Ο διαχωρισμός συνόλων σε υποσύνολα εκπαίδευσης και αξιολόγησης έγινε σε ποσοστά 60% και 40% αντίστοιχα. Το ποσοστό μη εισβολών σε κάθε σύνολο εκπαίδευσης και δοκιμασίας βρέθηκε παραπλήσιο, και κατά μέσο όρο ίσο με 80%.

Στα αποτελέσματα της υλοποίησης χρησιμοποιήθηκε ακρίβεια 3 δεκαδικών ψηφίων. Στα πεδία όπου υπάρχουν αλφαριθμητικές τιμές, έγινε αυτόματη μετατροπή σε δεκαδικούς (ξεκινώντας από τον αριθμό “0”) αριθμούς με σκοπό να είναι εφικτή η επεξεργασία των δεδομένων. Για την υλοποίηση αυτή, χρησιμοποιήθηκαν οι μοναδικές (unique) τιμές των χαρακτηριστικών, οι οποίες μετά αντικαταστάθηκαν. Έτσι, για παράδειγμα, πεδία όπως το “Label” με δυνατές τιμές

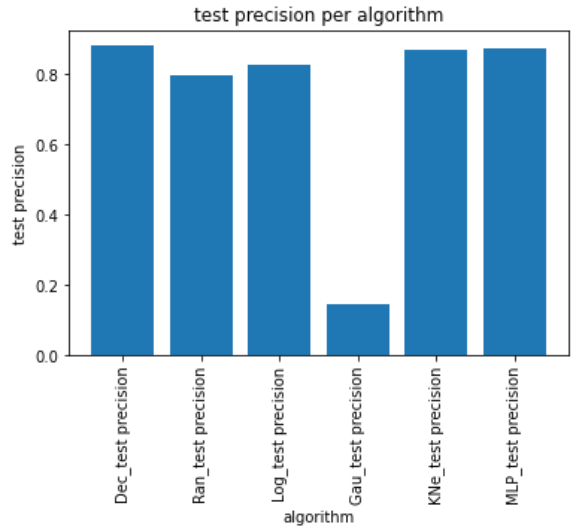
"Benign" και "Infiltration" απέκτησαν μετασχηματισμένες τιμές "0" και "1" αντίστοιχα. Για το σύνολο "cic-ids-2017" θεωρούμε εισβολή τις τιμές "FTP-Patator" και "SSH-Patator" (με εξαίρεση την περίπτωση που το σύνολο αυτό εκπαιδεύεται για τη δοκιμασία του "cic-ids-2019", όπου θεωρούμε εισβολή μόνο τις τιμές "FTP-Patator"). Για το σύνολο "cic-ids-2019" θεωρείται εισβολή η τιμή "TFTP". Στα σενάρια, στο πλαίσιο της ταξινόμησης, δοκιμάστηκαν οι αλγόριθμοι Decision Tree, Random Forest, Logistic Regression, Gaussian Naive Bayes, KNN, MLP και SVM.

4.2 Αποτελέσματα σεναρίου Α

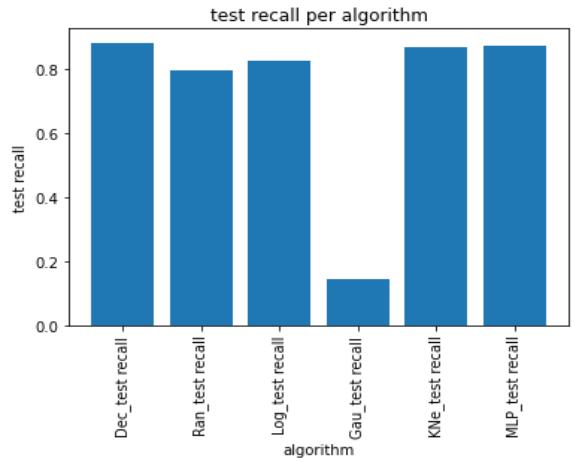
Σενάριο Α: Βήμα 1: Εκπαίδευση και αξιολόγηση μοντέλου με χρήση του συνόλου δεδομένων cic_ids2018_infiltration: Αποτελέσματα αλγορίθμων:



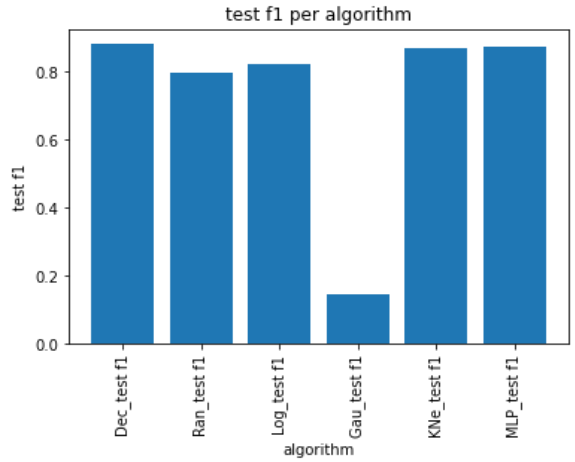
Αλγόριθμος	Accuracy
Decision Tree	0.881
Random Forest	0.795
Logistic Regression	0.824
Gaussian Naive Bayes	0.145
K-Nearest Neighbors	0.868
MLP	0.873



Αλγόριθμος	Precision
Decision Tree	0.881
Random Forest	0.795
Logistic Regression	0.824
Gaussian Naive Bayes	0.145
K-Nearest Neighbors	0.868
MLP	0.873



Αλγόριθμος	Recall
Decision Tree	0.881
Random Forest	0.795
Logistic Regression	0.824
Gaussian Naive Bayes	0.145
K-Nearest Neighbors	0.868
MLP	0.873



Αλγόριθμος	F1
Decision Tree	0.881
Random Forest	0.795
Logistic Regression	0.824
Gaussian Naive Bayes	0.145
K-Nearest Neighbors	0.868
MLP	0.873

Πίνακας 13: Αποτελέσματα αλγορίθμων στο βήμα 1 του σεναρίου Α.

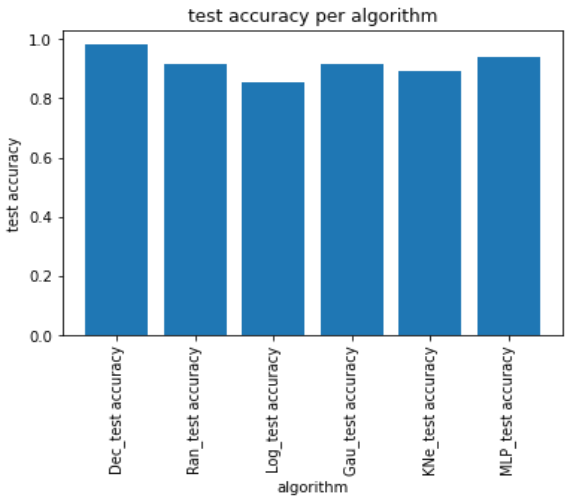
Αλγόριθμος	Χρόνος εκτέλεσης (σε δευτερόλεπτα)
DecisionTreeClassifier	15.731
RandomForestClassifier	27.123
LogisticRegression	19.160
GaussianNB	10.975
KNeighborsClassifier	1122.013
MLPClassifier	101.482
Σύνολο	1296.489

Πίνακας 14: Χρόνοι εκτέλεσης αλγορίθμων στο βήμα 1 του σεναρίου Α.

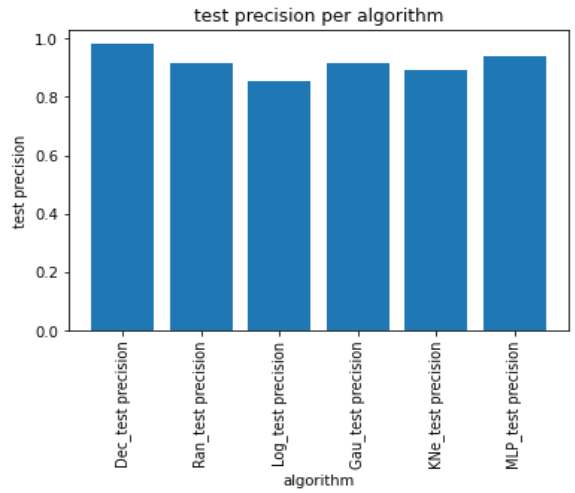
Στα αποτελέσματα του σεναρίου Α που αφορούν το βήμα 1, παρατηρήθηκαν ίδιες τιμές των μετρικών Accuracy, Precision, Recall και F1. Η βέλτιστη τιμή αυτών βρέθηκε στους αλγορίθμους Decision Tree, ίση με 0.881 (88.1%). Παραπλήσιες τιμές μετρικών βρέθηκαν στους αλγορίθμους MLP και KNN, στους οποίους αντιστοιχούς οι ίδιες μετρικές με τιμές 0.873 (87.3%) και 0.868 (86.8%) αντίστοιχα. Ο αλγόριθμος Gaussian Naive Bayes δεν σημείωσε καλές μετρικές (14.5%).

Ο Decision Tree αλγόριθμος για το συγκεκριμένο σύνολο στο οποίο έγινε η εκπαίδευση καθώς και η αξιολόγηση του μοντέλου cic_ids_2018_infiltration, αναδείχθηκε ταχύτερος από τους υπόλοιπους (15.731 sec). Επιλέχθηκε ο Decision Tree ως ο πιο αποδοτικός αλγόριθμος για το σενάριο αυτό.

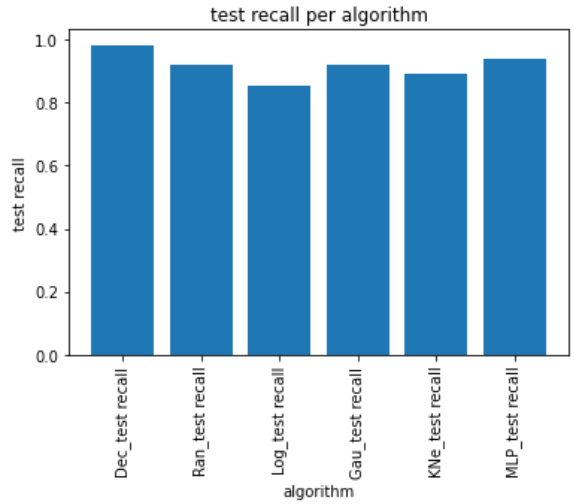
Σενάριο Α: Βήμα 2:
Εκπαίδευση και αξιολόγηση μοντέλου με χρήση του συνόλου δεδομένων cic_ids_2017_infiltration: Αποτελέσματα αλγορίθμων:



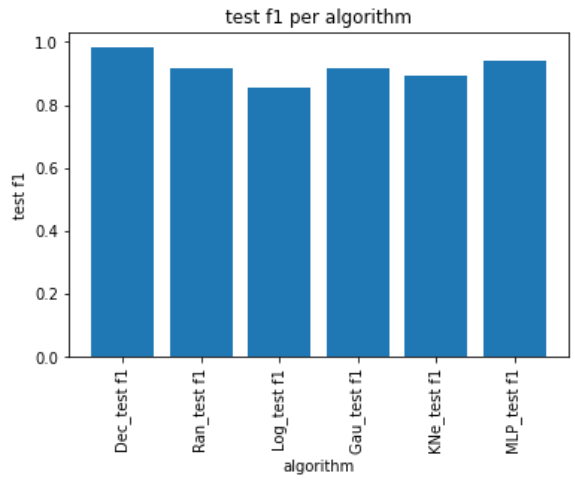
Αλγόριθμος	Accuracy
Decision Tree	0.982
Random Forest	0.918
Logistic Regression	0.853
Gaussian Naive Bayes	0.918
K-Nearest Neighbors	0.891
MLP	0.938



Αλγόριθμος	Precision
Decision Tree	0.982
Random Forest	0.918
Logistic Regression	0.853
Gaussian Naive Bayes	0.918
K-Nearest Neighbors	0.891
MLP	0.938



Αλγόριθμος	Recall
Decision Tree	0.982
Random Forest	0.918
Logistic Regression	0.853
Gaussian Naive Bayes	0.918
K-Nearest Neighbors	0.891
MLP	0.938



Αλγόριθμος	F1
Decision Tree	0.982
Random Forest	0.918
Logistic Regression	0.853
Gaussian Naive Bayes	0.918
K-Nearest Neighbors	0.891
MLP	0.938

Πίνακας 15: Αποτελέσματα αλγορίθμων στο βήμα 2 του σεναρίου Α.

Αλγόριθμος	Χρόνος εκτέλεσης (σε δευτερόλεπτα)
DecisionTreeClassifier	9.026
RandomForestClassifier	15.189
LogisticRegression	12.279
GaussianNB	8.124
KNeighborsClassifier	384.630
MLPClassifier	47.390
Σύνολο	476.644

Πίνακας 16: Χρόνοι εκτέλεσης αλγορίθμων στο βήμα 2 του σεναρίου Α.

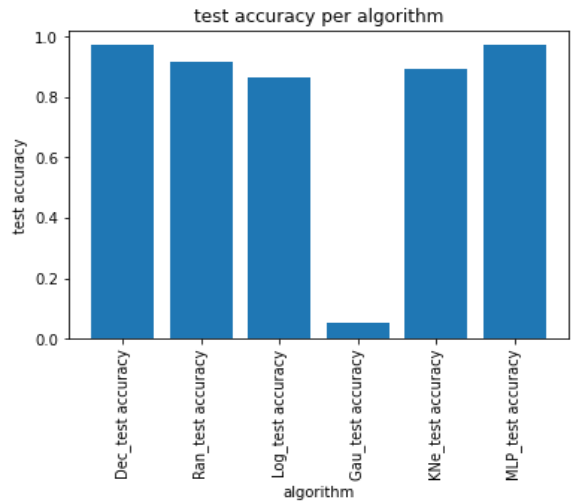
Στα αποτελέσματα του σεναρίου Α που αφορούν το βήμα 2, παρατηρήθηκαν ίδιες τιμές των μετρικών Accuracy, Precision, Recall και F1. Η βέλτιστη τιμή αυτών βρέθηκε στον αλγόριθμο Decision Tree, ίση με 0.982 (98.2%). Για το βήμα αυτό, ο Gaussian Naive Bayes αλγόριθμος αποδείχθηκε ταχύτερος από όλους τους υπόλοιπους (8.124 sec), ενώ ο Decision Tree εκτελέστηκε σε παραπλήσιο χρονικό πλαίσιο 9.026 (9.026 sec).

Παραπλήσιες υψηλές μετρικές βρέθηκαν στους αλγορίθμους Random Forest (91.8%), Gaussian Naive Bayes (91.8%) και MLP (93.8%), ενώ τις συγκριτικά χαμηλότερες απέδωσαν οι αλγόριθμοι Logistic Regression (85.3%) και KNN (89.1%).

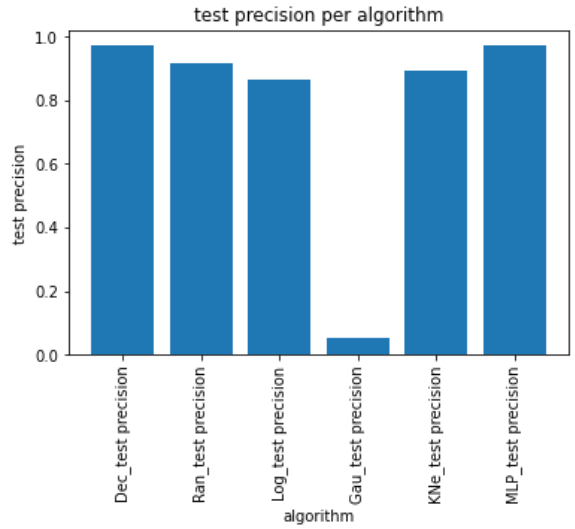
Επιλέχθηκε ο αλγόριθμος Decision Tree ως ο πιο αποδοτικός στο πλαίσιο της εκπαίδευσης και αξιολόγησης μοντέλου με βάση το σύνολο δεδομένων cic_ids_2017_infiltration.

Παρατηρήθηκε πως στο τρέχον βήμα αναγνωρίστηκε ο Decision Tree αλγόριθμος, κάτι που συνέβη και στο βήμα 1 του ίδιου σεναρίου.

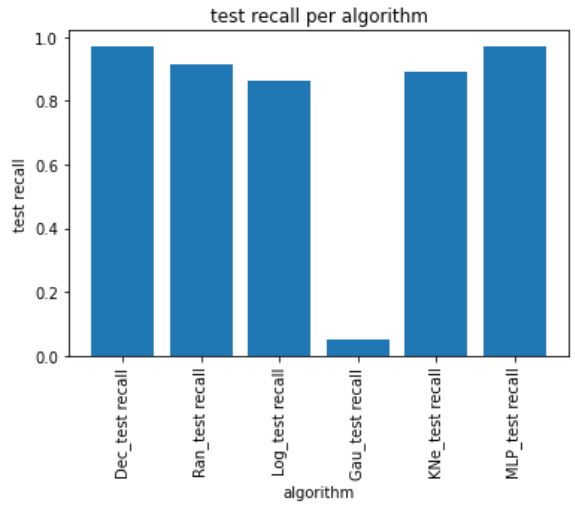
Σενάριο Α: Βήμα 3:
Εκπαίδευση του συνόλου δεδομένων cic_ids_2018_infiltration και αξιολόγηση μοντέλου με χρήση το σύνολο δεδομένων cic_ids_2017_infiltration: Αποτελέσματα αλγορίθμων:



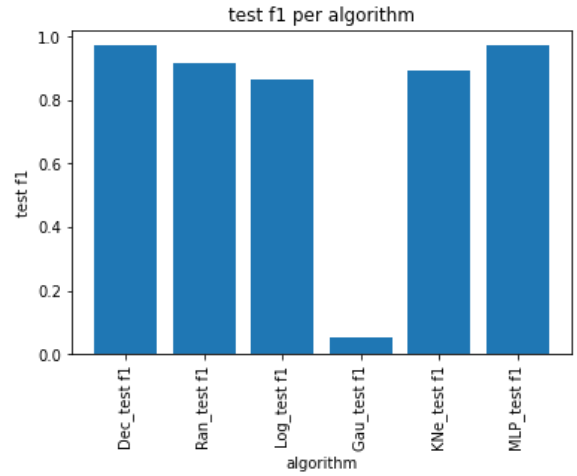
Αλγόριθμος	Accuracy
Decision Tree	0.972
Random Forest	0.915
Logistic Regression	0.863
Gaussian Naive Bayes	0.053
K-Nearest Neighbors	0.891
MLP	0.972



Αλγόριθμος	Precision
Decision Tree	0.972
Random Forest	0.915
Logistic Regression	0.863
Gaussian Naive Bayes	0.053
K-Nearest Neighbors	0.891
MLP	0.972



Αλγόριθμος	Recall
Decision Tree	0.972
Random Forest	0.915
Logistic Regression	0.863
Gaussian Naive Bayes	0.053
K-Nearest Neighbors	0.891
MLP	0.972



Αλγόριθμος	F1
Decision Tree	0.972
Random Forest	0.915
Logistic Regression	0.863
Gaussian Naive Bayes	0.053
K-Nearest Neighbors	0.891
MLP	0.972

Πίνακας 17: Αποτελέσματα αλγορίθμων στο βήμα 3 του σεναρίου Α.

Αλγόριθμος	Χρόνος εκτέλεσης (σε δευτερόλεπτα)
DecisionTreeClassifier	14.018
RandomForestClassifier	37.861
LogisticRegression	20.466
GaussianNB	9.032
KNeighborsClassifier	645.710
MLPClassifier	88.592
Σύνολο	1975.078

Πίνακας 18: Χρόνοι εκτέλεσης αλγορίθμων στο βήμα 3 του σεναρίου Α.

Στα αποτελέσματα του σεναρίου Α που αφορούν το βήμα 3, παρατηρήθηκαν ίδιες τιμές των μετρικών Accuracy, Precision, Recall και F1. Η βέλτιστη τιμή αυτών βρέθηκε στους αλγόριθμους Decision Tree και MLP, ίση με 0.972 (97.2%). Ο Gaussian Naive Bayes αλγόριθμος ως ταχύτερος από όλους τους υπόλοιπους (9.032 sec), βρέθηκε να έχει τις χαμηλότερες μετρικές (5.3%). Ο Decision Tree εκτελέστηκε σε χρονικό πλαίσιο 14.018 sec. Το γεγονός ότι ισοβάθμισαν οι μετρικές στους αλγορίθμους οφείλεται στο ότι το πλήθος των

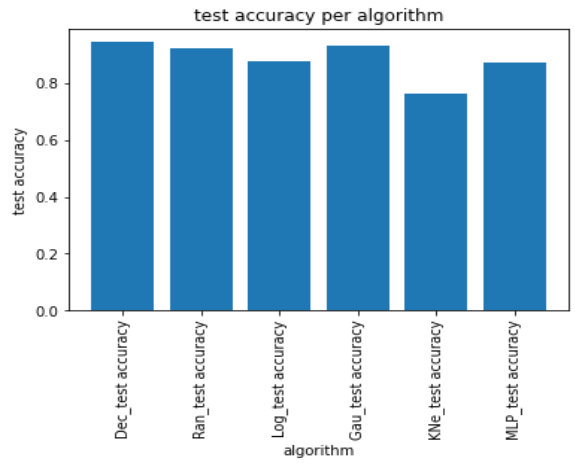
αληθώς θετικών είναι παραπλήσιος. Παραπλήσιες υψηλές μετρικές βρέθηκαν στους αλγορίθμους Random Forest και KNN.

Συγκρίνοντας τα αποτελέσματα των βημάτων 2 και 3 για το σενάριο Α, παρατηρείται πως ο αλγόριθμος Decision Tree (κατά κύριο λόγο) καθώς και ο MLP, αντιστιχούν στις καλύτερες μετρικές και στα δύο αυτά βήματα. Επίσης, συγκρίνοντας τα αποτελέσματα των δύο αυτών βημάτων, φάνηκε πως η απόδοση των αλγορίθμων Decision Tree, Random Forest, Gaussian Naive Bayes είναι μικρότερη στην περίπτωση που δοκιμάζονται σε διαφορετικό μοντέλο (βήμα 3) από αυτό που έγινε η εκπαίδευση, σε σχέση με την περίπτωση που ο μοντέλο εκπαιδεύτηκε και αξιολογήθηκε στο ίδιο σύνολο (βήμα 2). Το αντίθετο ισχύει για τους αλγορίθμους Logistic Regression και MLP, όπου η απόδοση των αλγορίθμων αυξήθηκε, ενώ στην περίπτωση του KNN, η απόδοση παρέμεινε η ίδια.

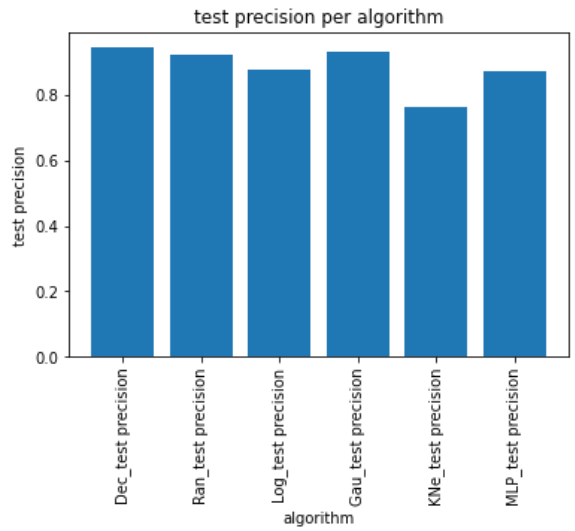
Στο σενάριο Α, αξιολογήθηκε ως αποδοτικότερος αλγόριθμος ο Decision Tree, καθώς έχει τις καλύτερες μετρικές Accuracy, Precision, Recall και F1. Αντίστοιχα, ο λιγότερο αποδοτικός παρατηρήθηκε πως είναι ο αλγόριθμος Gaussian Naive Bayes. Αυτό εξηγείται από το γεγονός ότι η Naive Bayes υπόθεση αναφέρει πως τα χαρακτηριστικά ενός συνόλου δεδομένων πρέπει να είναι ανεξάρτητα ώστε να είναι δυνατή η εκπαίδευση του μοντέλου.

4.3 Αποτελέσματα σεναρίου Β

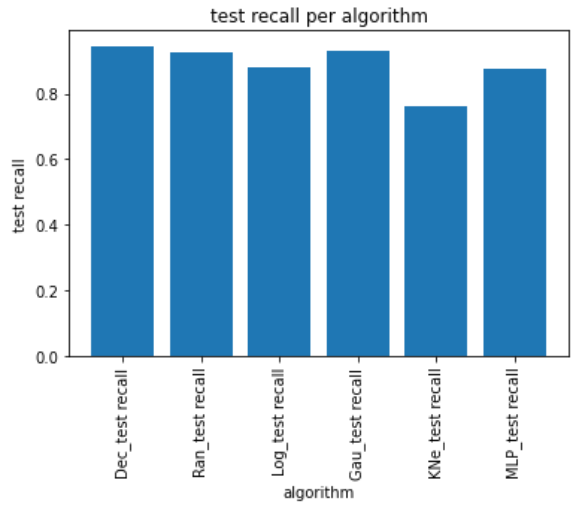
Σενάριο Β: Βήμα 1:
Εκπαίδευση και αξιολόγηση μοντέλου με χρήση του συνόλου δεδομένων cic_ids_2018_ftp_and_ssh_brute_force: Αποτελέσματα αλγορίθμων:



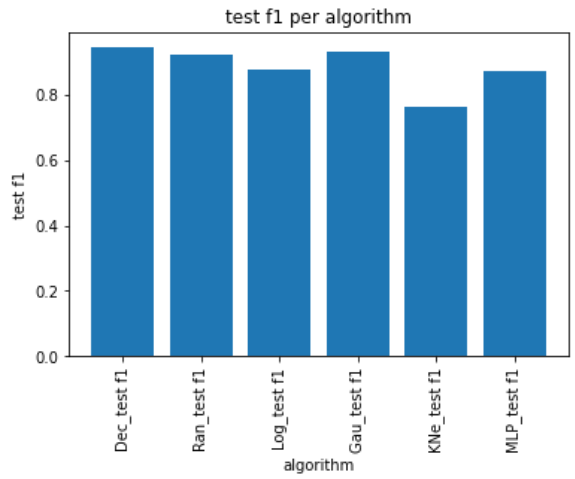
Αλγόριθμος	Accuracy
Decision Tree	0.945
Random Forest	0.924
Logistic Regression	0.879
Gaussian Naive Bayes	0.931
K-Nearest Neighbors	0.762
MLP	0.874



Αλγόριθμος	Precision
Decision Tree	0.945
Random Forest	0.924
Logistic Regression	0.879
Gaussian Naive Bayes	0.931
K-Nearest Neighbors	0.762
MLP	0.874



Αλγόριθμος	Recall
Decision Tree	0.945
Random Forest	0.924
Logistic Regression	0.879
Gaussian Naive Bayes	0.931
K-Nearest Neighbors	0.762
MLP	0.874



Αλγόριθμος	F1
Decision Tree	0.945
Random Forest	0.924
Logistic Regression	0.879
Gaussian Naive Bayes	0.931
K-Nearest Neighbors	0.762
MLP	0.874

Πίνακας 19: Αποτελέσματα αλγορίθμων στο βήμα 1 του σεναρίου Β.

Αλγόριθμος	Χρόνος εκτέλεσης (σε δευτερόλεπτα)
DecisionTreeClassifier	17.901
RandomForestClassifier	37.341
LogisticRegression	31.495
GaussianNB	15.829
KNeighborsClassifier	1929.113
MLPClassifier	69.182
Σύνολο	2100.868

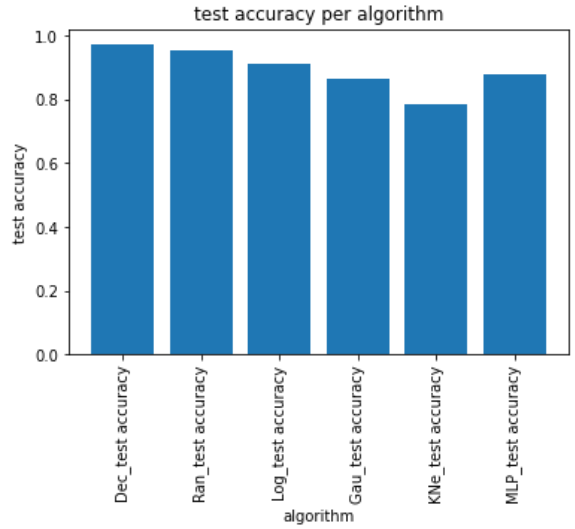
Πίνακας 20: Χρόνοι εκτέλεσης αλγορίθμων στο βήμα 1 του σεναρίου Β.

Στο βήμα 1 του δεύτερου σεναρίου, ο αλγόριθμοι Decision Tree παρατηρήθηκε πως έχει τις μεγαλύτερες μετρικές (99.9%) Accuracy, Precision, Recall και F1 σε σχέση με τους άλλους αλγορίθμους στο πλαίσιο της εκπαίδευσης και αξιολόγησης του συνόλου cic_ids_2018_ftp_and_ssh_brute_force.

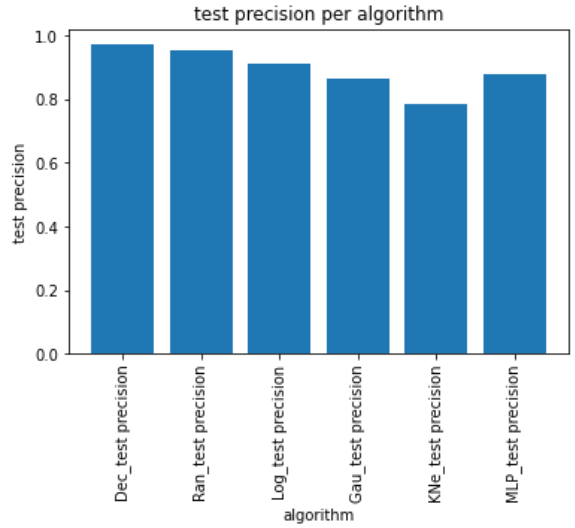
Παρόμοιες υψηλές τιμές στις μετρικές σημειώθηκαν από τους αλγορίθμους Random Forest, Gaussian Naive Bayes, με τιμές 92.4% και 93.1% αντίστοιχα. Συγκριτικά χαμηλές μετρικές απέδωσαν οι αλγόριθμοι KNN (76.2%), Logistic Regression (87.9%) και MLP (87.4%).

Ο Gaussian Naive Bayes σημείωσε τον συντομότερο χρόνο εκτέλεσης (15.829 sec), τιμή που βρίσκεται κοντά στον χρόνο εκτέλεσης του Decision Tree (17.901 sec), ενώ ο MLP είναι ο περισσότερο χρονοβόρος.

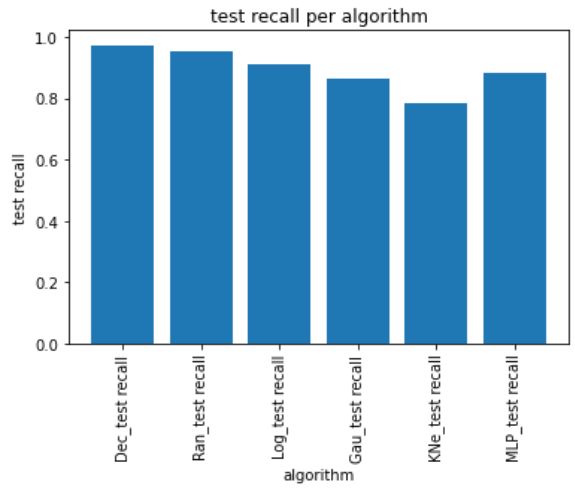
Σενάριο Β: Βήμα 2:
Εκπαίδευση και αξιολόγηση μοντέλου με χρήση του συνόλου δεδομένων cic_ids_2017_ftp_and_ssh_patators: Αποτελέσματα αλγορίθμων:



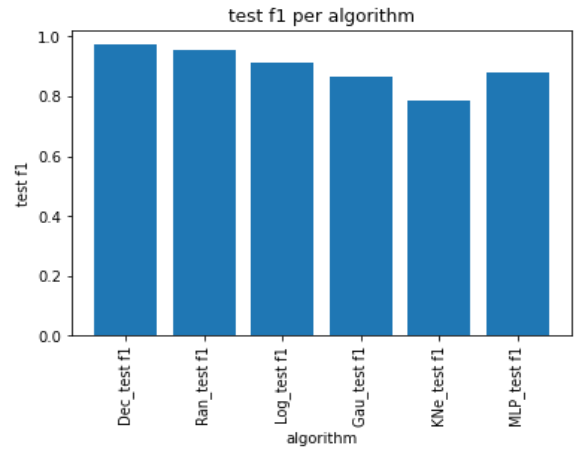
Αλγόριθμος	Accuracy
Decision Tree	0.973
Random Forest	0.955
Logistic Regression	0.912
Gaussian Naive Bayes	0.865
K-Nearest Neighbors	0.784
MLP	0.881



Αλγόριθμος	Precision
Decision Tree	0.973
Random Forest	0.955
Logistic Regression	0.912
Gaussian Naive Bayes	0.865
K-Nearest Neighbors	0.784
MLP	0.881



Αλγόριθμος	Recall
Decision Tree	0.973
Random Forest	0.955
Logistic Regression	0.912
Gaussian Naive Bayes	0.865
K-Nearest Neighbors	0.784
MLP	0.881



Αλγόριθμος	F1
Decision Tree	0.973
Random Forest	0.955
Logistic Regression	0.912
Gaussian Naive Bayes	0.865
K-Nearest Neighbors	0.784
MLP	0.881

Πίνακας 21: Αποτελέσματα αλγορίθμων στο βήμα 2 του σεναρίου Β.

Αλγόριθμος	Χρόνος εκτέλεσης (σε δευτερόλεπτα)
DecisionTreeClassifier	14.689
RandomForestClassifier	26.183
LogisticRegression	21.557
GaussianNB	13.556
KNeighborsClassifier	1012.714
MLPClassifier	61.288
Σύνολο	1149.988

Πίνακας 22: Χρόνοι εκτέλεσης αλγορίθμων στο βήμα 2 του σεναρίου Β.

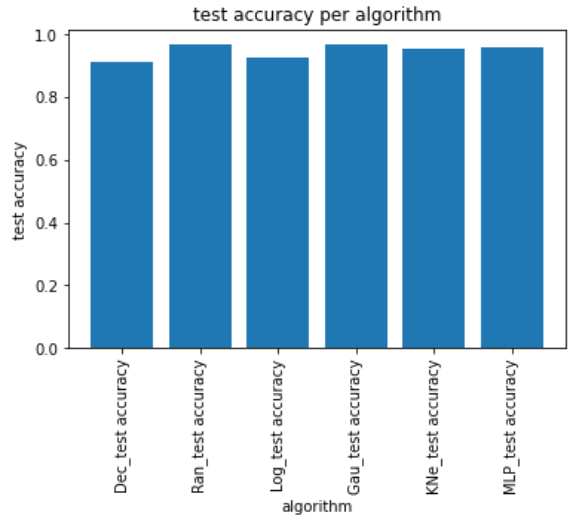
Στο δεύτερο βήμα του σεναρίου Β, στην αξιολόγηση του συνόλου cic_ids_2017_ftp_and_ssh_patators, ο αλγόριθμος Decision Tree σημείωσε τις καλύτερες μετρικές Accuracy, Precision, Recall και F1, με τιμή 0.973 (97.3%).

Παραπλήσιες υψηλές επιδόσεις βρέθηκαν από τους αλγορίθμους Random Forest και Logistic Regression, με τιμές μετρικών 95.5% και 91.2% αντίστοιχα. Χαμηλές μετρικές παρουσιάστηκαν στους αλγορίθμους KNN, Gaussian Naive Bayes και MLP. Συμπεριλαμβάνοντας το βήμα 1 του ίδιου σεναρίου, παρατηρήθηκε πως και στα δύο βήματα

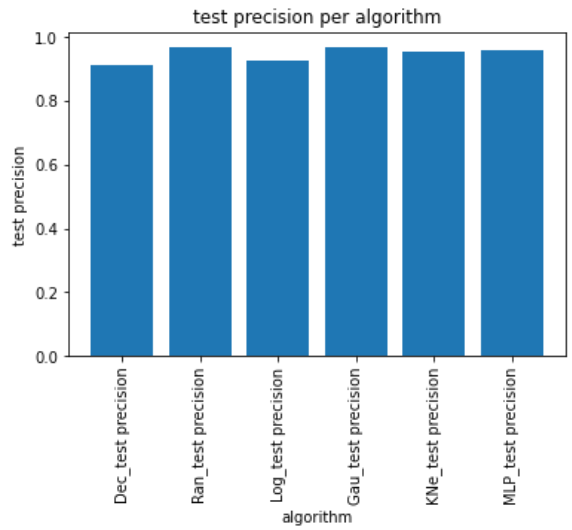
αυτά, ο Decision Tree είναι γενικότερα αποδοτικός προσφέροντας τις υψηλότερες μετρικές, και ακολουθεί ο αλγόριθμος Random Forest. Και στα δύο αυτά βήματα, τις χαμηλότερες τιμές έχουν οι αλγόριθμοι KNN και MLP.

Οι αλγόριθμοι Gaussian Naive Bayes και Decision Tree βρέθηκε πως έχουν τους μικρότερους χρόνους εκτέλεσης.

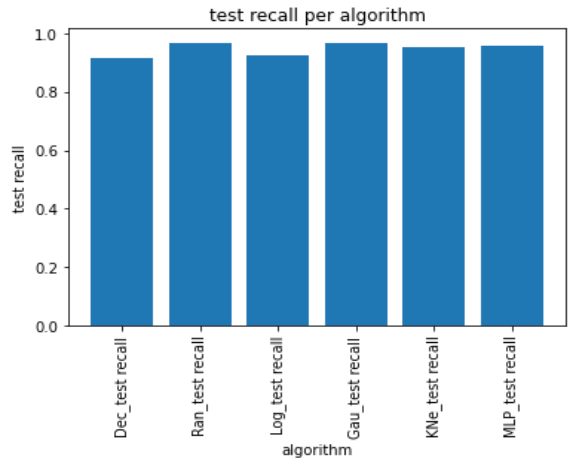
Σενάριο Β: Βήμα 3:
Εκπαίδευση του συνόλου δεδομένων cic_ids_2018_ftp_and_ssh_brute_force και αξιολόγηση μοντέλου με χρήση το σύνολο δεδομένων cic_ids_2017_ftp_and_ssh_patators:
Αποτελέσματα αλγορίθμων:



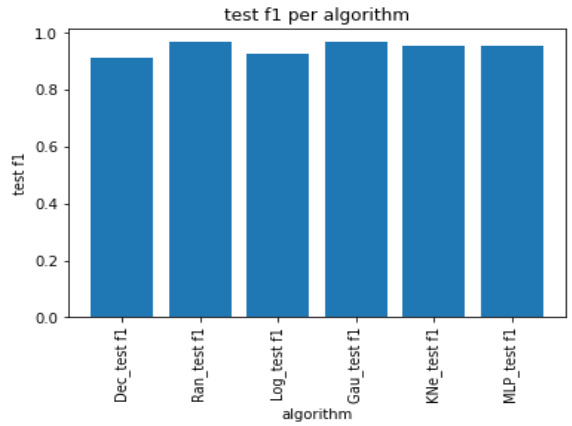
Αλγόριθμος	Accuracy
Decision Tree	0.914
Random Forest	0.968
Logistic Regression	0.927
Gaussian Naive Bayes	0.968
K-Nearest Neighbors	0.954
MLP	0.957



Αλγόριθμος	Precision
Decision Tree	0.914
Random Forest	0.968
Logistic Regression	0.927
Gaussian Naive Bayes	0.968
K-Nearest Neighbors	0.954
MLP	0.957



Αλγόριθμος	Recall
Decision Tree	0.914
Random Forest	0.968
Logistic Regression	0.927
Gaussian Naive Bayes	0.968
K-Nearest Neighbors	0.954
MLP	0.957



Αλγόριθμος	F1
Decision Tree	0.914
Random Forest	0.968
Logistic Regression	0.927
Gaussian Naive Bayes	0.968
K-Nearest Neighbors	0.954
MLP	0.957

Πίνακας 23: Αποτελέσματα αλγορίθμων στο βήμα 3 του σεναρίου Β.

Αλγόριθμος	Χρόνος εκτέλεσης (σε δευτερόλεπτα)
DecisionTreeClassifier	17.486
RandomForestClassifier	41.473
LogisticRegression	29.111
GaussianNB	14.538
KNeighborsClassifier	1782.404
MLPClassifier	90.057
Σύνολο	1975.078

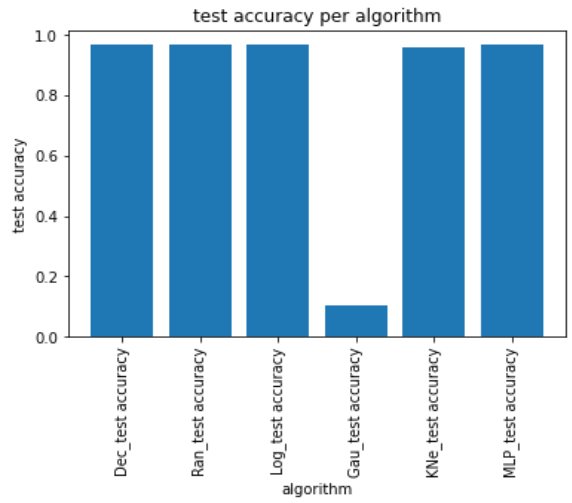
Πίνακας 24: Χρόνοι εκτέλεσης αλγορίθμων στο βήμα 3 του σεναρίου Β.

Στο τρίτο βήμα του σεναρίου Β, οι αλγόριθμοι Random Forest και Gaussian Naive Bayes σημείωσαν τις καλύτερες μετρικές Accuracy, Precision, Recall και F1, με τιμή 0.968 (96.8%), στο πλαίσιο της εκπαίδευσης μοντέλου με βάση το σύνολο cic_ids_2018_ftp_and_ssh_brute_force, και αξιολόγηση με χρήση του μοντέλου cic_ids_2017_ftp_and_ssh_patators.

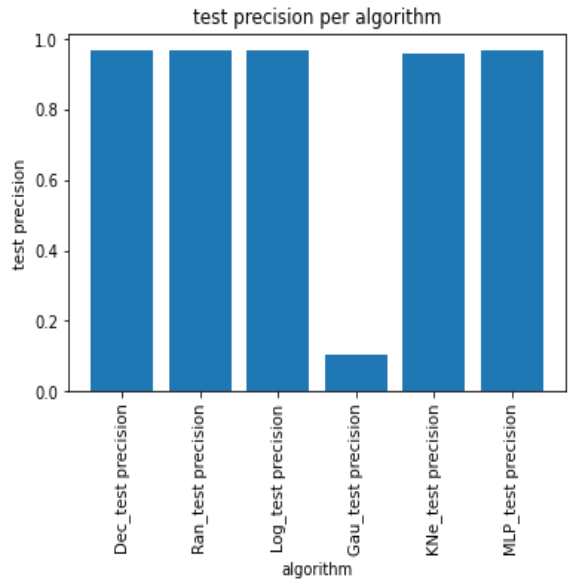
Οι Gaussian Naive Bayes και Decision Tree αποδείχθηκαν ταχύτεροι από τους υπόλοιπους. Στο σενάριο Β, ο αλγόριθμος Random Forest φάνηκε πως έχει τις υψηλότερες μετρικές, και επιλέχθηκε ως ο πιο αποδοτικός για το συγκεκριμένο σενάριο, σε αντίθεση με το σενάριο Α όπου επιλέχθηκε ο αλγόριθμος Decision Tree. Συγκρίνοντας τα αποτελέσματα των βημάτων 2 και 3 για το σενάριο Β, παρατηρήθηκε πως ο αλγόριθμος Decision Tree μείωσε την αποδοτικότητά του κατά την δοκιμασία μοντέλου σε διαφορετικό σύνολο (βήμα 3), σε σχέση με την περίπτωση που δοκιμάστηκε στο ίδιο σύνολο που έγινε η εκπαίδευση (βήμα 2). Το αντίθετο συνέβη στους υπόλοιπους αλγορίθμους, οι οποίοι αύξησαν την αποδοτηκότητά τους.

4.4 Αποτελέσματα σεναρίου Γ

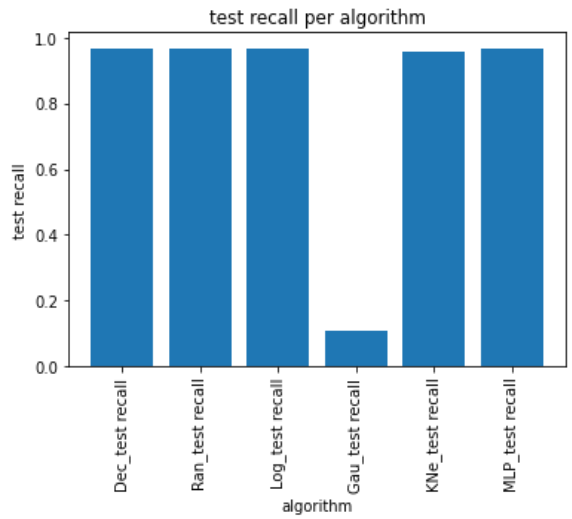
Σενάριο Γ: Βήμα 1:
Εκπαίδευση του συνόλου δεδομένων cic_ids_2018_infiltration και αξιολόγηση μοντέλου με χρήση το σύνολο δεδομένων cic_ids_2017_ftp_and_ssh_patators: Αποτελέσματα αλγορίθμων:



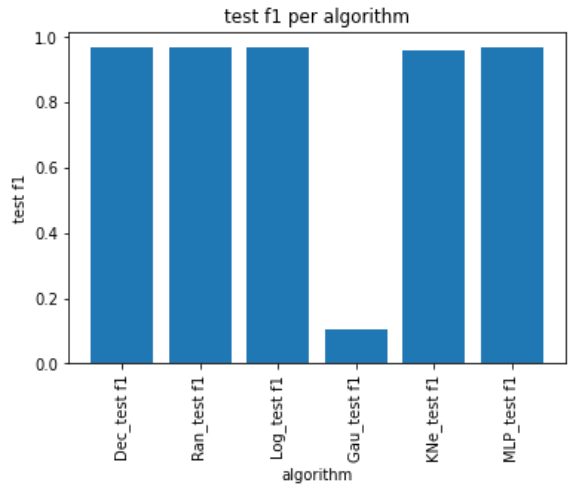
Αλγόριθμος	Accuracy
Decision Tree	0.968
Random Forest	0.968
Logistic Regression	0.967
Gaussian Naive Bayes	0.105
K-Nearest Neighbors	0.958
MLP	0.968



Αλγόριθμος	Precision
Decision Tree	0.968
Random Forest	0.968
Logistic Regression	0.967
Gaussian Naive Bayes	0.105
K-Nearest Neighbors	0.958
MLP	0.968



Αλγόριθμος	Recall
Decision Tree	0.968
Random Forest	0.968
Logistic Regression	0.967
Gaussian Naive Bayes	0.105
K-Nearest Neighbors	0.958
MLP	0.968



Αλγόριθμος	F1
Decision Tree	0.968
Random Forest	0.968
Logistic Regression	0.967
Gaussian Naive Bayes	0.105
K-Nearest Neighbors	0.958
MLP	0.968

Πίνακας 25: Αποτελέσματα αλγορίθμων στο βήμα 1 του σεναρίου Γ.

Αλγόριθμος	Χρόνος εκτέλεσης (σε δευτερόλεπτα)
DecisionTreeClassifier	14.621
RandomForestClassifier	26.645
LogisticRegression	20.036
GaussianNB	11.519
KNeighborsClassifier	1243.070
MLPClassifier	87.373
Σύνολο	1403.268

Πίνακας 26: Χρόνοι εκτέλεσης αλγορίθμων στο βήμα 1 του σεναρίου Γ.

Στο τρίτο σενάριο, τις καλύτερες τιμές σε Accuracy, Precision, Recall και F1 έδωσαν οι αλγόριθμοι Decision Tree, Random Forest και MLP. Ο μικρότερος χρόνος εκτέλεσης αντιστοιχήθηκε στον Decision Tree, λαμβάνοντας υπόψη πως ο Gaussian Naive Bayes δεν προσφέρει καλές μετρικές. Συνολικά επιλέχθηκε ο Decision Tree ως ο πιο αποδοτικός αλγόριθμος για το σενάριο που εκπαιδεύτηκε ένα μοντέλο με βάση το σύνολο δεδομένων cic_ids_2018_infiltration και δοκιμάστηκε στο σύνολο cic_ids_2017_ftp_and_ssh_patators.

Οι αλγόριθμοι Decision Tree και Random Forest φάνηκε πως ανταποκρίθηκαν με τις καλύτερες μετρικές Accuracy, Precision, Recall και F1 στα σενάρια Α, Β και Γ. Οι δύο αυτοί αλγόριθμοι απέδωσαν επαρκώς και στα σενάρια Α και Β. Ο αλγόριθμος MLP σημείωσε από τις καλύτερες μετρικές κατά την αξιολόγηση του τρίτου σεναρίου. Αξιολογώντας τη συμπεριφορά του αλγορίθμου Gaussian Naive Bayes και στα τρία σενάρια Α, Β και Γ, φάνηκε πως αδυνατεί να εφαρμοστεί αποδοτικά.

Κεφάλαιο 5: Σύνοψη

Στην διπλωματική αυτή εργασία έγινε ανάλυση των συστημάτων ανίχνευσης εισβολών, τα οποία διακρίνονται σε host based και network based. Η επιλογή του σωστού συστήματος, έχει πολλές παραμέτρους που πρέπει να ληφθούν υπόψη, όπως το κόστος, το λειτουργικό σύστημα που υποστηρίζεται, και οι ίδιες οι απαιτήσεις του χρήστη με σκοπό την κάλυψη αναγκών σε επίπεδο ασφαλείας host ή/και network.

Τα σύνολα δεδομένων που υπάρχουν στο διαδίκτυο, αποτελούν μία πρώτη μορφή στατικών αρχείων, τα οποία χρειάζονται ανάλυση και προεπεξεργασία, καθώς από μόνα τους δεν προσφέρουν ορατή πληροφορία. Στο σύνολό τους όμως, οι εγγραφές των συνόλων εμπεριέχουν πληροφορία για τα εκάστοτε χαρακτηριστικά που αντιστοιχούν, η οποία είναι χρήσιμη, και βοηθάει στην εκπαίδευση αποδοτικών μοντέλων μηχανικής μάθησης, τα οποία έχουν την ικανότητα να προβλέψουν σωστά την ανίχνευση εισβολών.

Ένας παράγοντας για την παραπάνω επιτυχία, εκτός της ανάλυσης και προεπεξεργασίας των συνόλων δεδομένων, αποτελεί και η σωστή χρήση αλγορίθμων μηχανικής μάθησης. Στο πλαίσιο της εργασίας αυτής, εξετάστηκαν οι αλγόριθμοι Gaussian Naive Bayes, KNN, MLP, Decision Tree, Random Forest και Logistic Regression, αναδείχθηκαν δυνατότητες και αδυναμίες αυτών στο πλαίσιο της εφαρμογής τους με σκοπό την επιβλεπόμενη μάθηση, και συγκεκριμένα την ταξινόμηση. Συνεπώς, αλγόριθμοι όπως ο Gaussian Naive Bayes που χρησιμοποιούν την υπόθεση πως τα χαρακτηριστικά είναι ανεξάρτητα μεταξύ τους, δίνουν χαμηλή ακρίβεια σε σύνολα δεδομένων που δεν ικανοποιούν την υπόθεση αυτή. Επίσης, το χαρακτηριστικό του χρόνου, δημιουργεί προβλήματα στην εκπαίδευση αλγορίθμων, και χρειάζεται διαφορετικούς τρόπους προσέγγισης. Εκτός από την επιλογή αλγορίθμων, χρειάζεται και βελτιστοποίηση αυτών κατά την χρήση τους, παραμετροποιώντας τους έτσι ώστε να υπάρχει βέλτιστο αποτέλεσμα, στην ποιότητα αποτελεσμάτων καθώς και στον χρόνο εκτέλεσης.

Οι προαναφερόμενοι αλγόριθμοι καθώς και τα υπάρχοντα συστήματα ανίχνευσης εισβολών που παρουσιάστηκαν, μπορούν να συνδυαστούν. Τα συστήματα αυτά παρέχουν εξόδους, σε μορφή αρχείων, τα οποία μπορούν να διαβάζονται, άρα και να αποτελούν είσοδο για ένα

πρόγραμμα στο οποίο εκτελούνται αλγόριθμοι μηχανικής μάθησης. Έτσι, είναι δυνατή η επιτήρηση ακόμα και σε πραγματικό, ανίχνευσης εισβολών από ένα σύστημα και από ένα υπολογιστικό πρόγραμμα/αλγόριθμο παράλληλα.

Συντομεύσεις

CGI: Common Gateway Interface (κοινή διεπαφή πύλης).

CPU: Central Processing Unit (κεντρική μονάδα επεξεργασίας).

DARPA: Defense Advanced Research Projects Agency (υπηρεσία έρευνας προηγμένων αμυντικών προγραμμάτων).

DNS: Domain Name System (σύστημα ονοματοδοσίας τομέων).

EHMS: Enhanced Healthcare Monitoring System (ενισχυμένο σύστημα παρακολούθησης υγειονομικής περίθαλψης).

FTP: File Transfer Protocol (πρωτόκολλο μεταφοράς αρχείων).

GUI: Graphical User Interface (γραφική διεπαφή χρήστη).

HIDS: Hosed-Based Intrusion Detection Systems (συστήματα ανίχνευσης εισβολής βασισμένα σε φιλοξενία).

HTTP: Hyper Text Transfer Protocol (πρωτόκολλο μεταφοράς υπερκειμένου).

IDS: Intrusion Detection System (σύστημα ανίχνευσης εισβολής).

IMAP: Internet Message Access Protocol (πρωτόκολλο πρόσβασης διαδικτυακών μηνυμάτων).

IOC: Indicators of Compromise (δείκτες συμβιβασμού).

IPS: Intrusion Prevention System (σύστημα εμπόδισης εισβολής).

ISMS: Information Security Management System (σύστημα διαχείρισης ασφάλειας πληροφοριών).

NIDS: Network-Based Intrusion Detection Systems (συστήματα ανίχνευσης εισβολής βασισμένα σε δίκτυο).

NSM: Network Security Monitoring (παρακολούθηση ασφάλειας δικτύου).

OS: Operating System (λειτουργικό σύστημα).

POP3: Post Office Protocol (πρωτόκολλο παραλαβής ηλεκτρονικών μηνυμάτων).

SIEM: Security Information and Event Management (πληροφορίες ασφαλείας και διαχείριση συμβάντων).

SNMP: Simple Network Management Protocol (απλό πρωτόκολλο διαχείρισης δικτύου).

SSH: Secure Shell Protocol (πρωτόκολλο ασφαλούς κελύφους).

TLS: Transport Layer Security (ασφάλεια επιπέδου μεταφοράς).

UDP: User Datagram Protocol (πρωτόκολλο μεταγωγής πακέτων χρήστη).

WIPS: Wireless Intrusion Prevention System (ασύρματο σύστημα εμπόδισης εισβολής).

Αναφορές

[1]Udemy Course online data science and machine learning with Python hands on https://www.udemy.com/course/data-science-and-machine-learning-with-python-hands-on/learn/lecture/15089750#overview

[2]Burr, Thomas. "Pattern Recognition and Machine Learning. Christopher M. Bishop." Journal of the American Statistical Association 103 (2008): 886-887, Ch 1. Introduction.

[3]Burr, Thomas. "Pattern Recognition and Machine Learning. Christopher M. Bishop." Journal of the American Statistical Association 103 (2008): 886-887. Ch. 1.1 Example: Polynomial Curve Fitting).

[4]Supervised vs. Unsupervised Learning and use cases for each https://medium.com/@dkatzman_3920/supervised-vs-unsupervised-learning-and-use-cases-for-each-8b9cc3ebd301

[5]William, Stallings. Computer security: Principles and practice, Ch. 1.1. Pearson Education India, 2008.

[6]William, Stallings. Computer security: Principles and practice, Ch. 1.2. Pearson Education India, 2008.

[7]William, Stallings. Computer security: Principles and practice, Ch. 8. Pearson Education India, 2008.

[8]Intrusion Detection Systems Explained: 14 Best IDS Software Tools Reviewed https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

[9]8 Types of Health Information Technology & Healthcare Software System https://www.softwaresuggest.com/blog/types-of-health-information-technology-and-healthcare-software/

[10]Machine learning approaches https://en.wikipedia.org/wiki/Machine_learning#Approaches

[11]Pattern recognition algorithms https://en.wikipedia.org/wiki/Pattern_recognition#Algorithms

[12]5 open source intrusion detection systems for smbs https://www.csoonline.com/article/3596315/5-open-source-intrusion-detection-systems-for-smbs.html

[13]Server Message Block https://en.wikipedia.org/wiki/Server_Message_Block

[14]5 open source nids https://logz.io/blog/5-open-source-nids/

[15]5 open source intrusion detection tools that are too good to ignore https://towerwall.com/5-open-source-intrusion-detection-tools-that-are-too-good-to-ignore/

[16]Zeek Bro support https://logz.io/blog/zeek-bro-support/

[17]OSSEC overview https://apps.splunk.com/app/300/

[18]Security Onion Peel Back the Layers of Your Enterprise https://blog.securityonion.net/2018/07/security-onion-160443-now-available.html

[19]10 WiFi security tools for your arsenal, Kismet https://www.computerweekly.com/photostory/2240146794/10-Wi-Fi-security-tools-for-your-arsenal/3/2-Kismet

[20]Survey of intrusion detection systems: techniques, datasets and challenges https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

[21] Koziol, Jack. Intrusion detection with Snort. Sams Publishing, 2003.

[22]Intrusion Detection Evaluation Dataset (CIC-IDS2017) https://www.unb.ca/cic/datasets/ids-2017.html

[23]Data exfiltration https://en.wikipedia.org/wiki/Data_exfiltration

[24]Host based intrusion detection systems https://www.dnsstuff.com/host-based-intrusion-detection-systems

[25]Snort manual website subsections http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node21.html

[26]Intrusion detection system using machine learning algorithms https://www.geeksforgeeks.org/intrusion-detection-system-using-machine-learning-algorithms/

[27]A Deeper Dive into the NSL-KDD Data Set https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657

[28]A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection https://www.researchgate.net/figure/LITNET-2020-dataset-features-list-with-descriptions_tbl5_343695445

[29]Hady, Anar A., et al. "Intrusion detection system for healthcare systems using medical and network data: A comparison study." IEEE Access 8 (2020): 106576-106584. https://ieeexplore.ieee.org/document/9109651

[30]WUSTL EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity Research https://www.cse.wustl.edu/~jain/ehms/index.html

[31]Argus, https://openargus.org.

[32]LITNET-2020: An Annotated Real-World Network Flow Dataset for Network Intrusion Detection https://www.mdpi.com/2079-9292/9/5/800

[33]Tavallaee, Mahbod, et al. "A detailed analysis of the KDD CUP 99 data set." 2009 IEEE symposium on computational intelligence for security and defense applications. Ieee, 2009.

[34]McHugh, John. "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory." ACM Transactions on Information and System Security (TISSEC) 3.4 (2000): 262-294.

[35]IoT device network logs https://www.kaggle.com/speedwall10/iot-device-network-logs

[36]SSH https://el.wikipedia.org/wiki/SSH

[37]Επίθεση Smurf https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_Smurf

[38]Snort manual configurations https://www.snort.org/configurations

[39]Snort rules default classification config https://www.apt-browse.org/browse/debian/wheezy/main/all/snort-rules-default/2.9.2.2-3/file/etc/snort/classification.config

[40]Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP https://www.semanticscholar.org/paper/signature based-Network-Intrusion-Detection-System-Shah-Singh/2e77c1af4ae2d1d855608f5711beb2b844866395

[41]OSSEC manual doc monitoring https://www.ossec.net/docs/docs/manual/monitoring/index.html

[42]OSSEC manual output https://www.ossec.net/docs/manual/output/index.html

[43]Roesch, Martin. "Snort Documents." (1998).

[44]IoT dataset for Intrusion Detection Systems (IDS) https://www.kaggle.com/azalhowaide/iot-dataset-for-intrusion-detection-systems-ids

[45]Alhowaide, Alaa, Izzat Alsmadi, and Jian Tang. "Pca, random-forest and pearson correlation for dimensionality reduction in iot ids." 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). IEEE, 2020.

[46]Alhowaide, Alsmadi, Tang. “An Ensemble Feature Selection Method for IoT IDS”, 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys), Fiji, Dec. 2020.

[47]A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015 https://www.researchgate.net/figure/The-relation-between-main-and-extracted-datasets-KDD99-is-created-from-DARPA-NSL-KDD-is_fig2_309038723

[48]Brute force attack https://el.wikipedia.org/wiki/Brute-force_attack

[49]LITNET-2020: an annotated real-world network flows dataset for network intrusion detection. https://dataset.litnet.lt

[50]Sharafaldin, Iman, Arash Habibi Lashkari, and Ali A. Ghorbani. "Toward generating a new intrusion detection dataset and intrusion traffic characterization." ICISSp 1 (2018): 108-116.

[51]Προγραμματιστικά Εργαλεία και Τεχνολογίες για Επιστήμη Δεδομένων, Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών. Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών https://courses.softlab.ntua.gr/progds/2021b/

[52]Kaggle dataset CIC-IDS-2018_Preprocessed https://www.kaggle.com/datasets/shixinliu/cicids2018-preprocessed

[53]Kaggle dataset sampled tft pattack cic ddos 2019, https://www.kaggle.com/datasets/pedrohauy/sampledtftpattackcicddos2019

[55]Ye, Nong, et al. "Probabilistic techniques for intrusion detection based on computer audit data." IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans 31.4 (2001): 266-274.

[56]Sharafaldin, Iman, et al. "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy." 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019.

[57]DDoS Evaluation Dataset (CIC-DDoS2019) https://www.unb.ca/cic/datasets/ddos-2019.html

[58] CSE-CIC-IDS2018 on AWS https://www.unb.ca/cic/datasets/ids-2018.html

[59]Perfect Recipe for Classification Using Logistic Regression https://towardsdatascience.com/the-perfect-recipe-for-classification-using-logistic-regression-f8648e267592

[60]Perceptron https://el.wikipedia.org/wiki/Perceptron

[61]Βασικές αρχές εκπαίδευσης ΤΝΔ (Τεχνιτών Νευρωνικών Δικτύων): Το perceptron https://www.cs.uoi.gr/~arly/courses/nn/slides/K2.pdf

[62]Μοντέλο Perceptron πολλών στρωμάτων Multi Layer Perceptron (MLP) https://docplayer.gr/60744858-Montelo-perceptron-pollon-stromaton-multi-layer-perceptron-mlp.html

[64]Decision tree learning https://en.wikipedia.org/wiki/Decision_tree_learning

[65]Δέντρα Απόφασης (Decision Trees) https://www.ceid.upatras.gr/webpages/courses/cplusplus/dm/decision_trees1.pdf

[66]Random Forest https://en.wikipedia.org/wiki/Random_forest

[67]Understanding Random Forest https://www.analyticsvidhya.com/blog/2021/06/understanding-random-forest/

[68]scikit-learn Machine Learning in Python https://scikit-learn.org/stable/

[69]Median https://en.wikipedia.org/wiki/Median

[70]Mean https://en.wikipedia.org/wiki/Mean

[71]Standard deviation https://en.wikipedia.org/wiki/Standard_deviation

[72]Variance https://en.wikipedia.org/wiki/Variance

[73]Supervised learning https://en.wikipedia.org/wiki/Supervised_learning

[74]Introducing the World's First Modern Cloud-Based SecOps Platform: Splunk Security Cloud https://www.splunk.com/en_us/blog/security/introducing-the-world-s-first-modern-cloud-based-secops-platform-splunk-security-cloud.html

[75]Basic snort rules syntax and usage [updated 2021] https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/

[76]An approach for anomaly based Intrusion detection system using Snort https://www.ijser.org/paper/An-approach-for-anomaly based-Intrusion-detection-System-using-SNORT.html

[77]Snort ACID: Installation and Configuration https://www.andrew.cmu.edu/user/rdanyliw/snort/acid_config.html

[78]Intrusion detection system http://en.wikipedia.org/wiki/Intrusion_detection_system