Τι είναι το Software-Defined Networking (SDN);

Η δικτύωση που ορίζεται από λογισμικό (SDN) είναι ένα παράδειγμα δικτύου που αποσυνδέει τα επίπεδα ελέγχου και δεδομένων από συσκευές δικτύου και τα τοποθετεί σε ξεχωριστές οντότητες. Στο SDN, η κίνηση δικτύου ελέγχεται από το λογισμικό που κατευθύνει την κίνηση μεταξύ των κεντρικών υπολογιστών. Αυτό είναι σε αντίθεση με την τρέχουσα αρχιτεκτονική δικτύου όπου ο έλεγχος κυκλοφορίας βασίζεται σε υλικό που ορίζεται από τους διακόπτες, τους δρομολογητές και άλλες υποδομές δικτύου.

Από τι αποτελείται το SDN;

Το SDN περιέχει τρία επίπεδα που περιλαμβάνουν (1) επίπεδο υποδομής (infrastructure layer), (2) επίπεδο ελέγχου (control layer), (3) επίπεδο εφαρμογής (application layer). Το επίπεδο υποδομής περιλαμβάνει συσκευές δικτύου, οι οποίες διαβιβάζουν τα ληφθέντα πακέτα σύμφωνα με τις οδηγίες από τον ελεγκτή SDN. Υπάρχουν διαφορετικές εφαρμογές SDN στο επίπεδο εφαρμογής, οι οποίες λαμβάνουν αποφάσεις σχετικά με τον τρόπο αντιμετώπισης των πακέτων που λαμβάνονται από τους μεταγωγείς (switches). Το επίπεδο ελέγχου παρέχει τις πληροφορίες δικτύου στις εφαρμογές, μεταφράζει τις αποφάσεις που λαμβάνονται από τις εφαρμογές σε οδηγίες που μπορούν να γίνουν αποδεκτές από τους διακόπτες με δυνατότητα SDN και εκτελεί κάποιο βασικό έλεγχο και διαχείριση στις συσκευές δικτύου.

Οφελη SDN

Τα πλεονεκτήματα που σχετίζονται με το SDN περιλαμβάνουν (i) οι πολιτικές δικτύου ορίζονται από γλώσσες υψηλού επιπέδου στις εφαρμογές αντί για εντολές χαμηλού επιπέδου. (ii) η ανάπτυξη εφαρμογών είναι απλή, καθώς ο ελεγκτής παρέχει χρήσιμες αφαιρέσεις δικτύου, όπως προβολή καθολικού δικτύου, διαχείριση ροής, διαχείριση συσκευών και παρακολούθηση στατιστικών στοιχείων. (iii) οι συσκευές μεταγωγής γίνονται συσκευές πολλαπλών χρήσεων ακολουθώντας τους κανόνες ροής που παρέχονται από το επίπεδο ελέγχου.

Distributed Denial-of-Service (DDoS)

Η κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών (DDoS) είναι μια από τις πιο σοβαρές απειλές για την τρέχουσα ασφάλεια του δικτύου. Οι εισβολείς χρησιμοποιούν ένα botnet για να στείλουν τεράστια άχρηστα πακέτα, τα οποία θα εξαντλήσουν γρήγορα τους πόρους του στόχου, όπως εύρος ζώνης, μνήμη, CPU, κ.λπ. Σε σύγκριση με άλλες επιθέσεις, οι επιθέσεις DDoS έχουν διάφορες μεθόδους επίθεσης, μεγάλης κλίμακας κίνηση και κατανεμημένους μολυσμένους κεντρικούς υπολογιστές όλα αυτά καθιστούν πρόκληση την υπεράσπιση. Οι επιθέσεις DDoS μπορούν δυνητικά να προκαλέσουν σημαντική ζημιά. Για παράδειγμα, τον Μάρτιο του 2013, μια επίθεση DDoS κατά του Spamhaus προκάλεσε σημαντική συμφόρηση δικτύου, με αποτέλεσμα σημαντική απώλεια.

Security Flaws

Εκτός από τα πολυάριθμα οφέλη που προσφέρει το SDN, έχει ελαττώματα ασφαλείας που μπορούν να αξιοποιηθούν σε πολλαπλά αρχιτεκτονικά επίπεδα.

1) Επίπεδο εφαρμογής (*Application Plane)*: Η επίθεση πραγματοποιείται μέσω των εφαρμογών του επιπέδου εφαρμογής. Η αδίστακτη εφαρμογή εξαντλεί τους πόρους, θέτοντας νόμιμους χρήστες σε κίνδυνο.

2) Επίπεδο ελέγχου (*Control Plane)*: Ο εισβολέας κάνει μεγάλο αριθμό αιτημάτων από ψεύτικες διευθύνσεις IP, με αποτέλεσμα το Control Plane να επεξεργάζεται μεγάλο αριθμό Packet_IN μηνύματα. Προκαλεί καθυστέρηση ή απόρριψη του αιτήματος του νόμιμου χρήστη.

3) Επίπεδο υποδομής (*Data plane-infrastructure layer)*: Ο εισβολέας μπορεί να επιτεθεί στο επίπεδο δεδομένων πλημμυρίζοντας τον πίνακα ροής του διακόπτη, με αποτέλεσμα μια επίθεση υπερχείλισης του πίνακα ροής.

Proposed Approach

Η προτεινόμενη λύση αποτελείται από δύο μέρη. Η πρώτη ενότητα για την κατασκευή του συνόλου δεδομένων, συλλέγει στατιστικά στοιχεία, ενώ η δεύτερη ενότητα χρησιμοποιεί μια τεχνική μηχανικής μάθησης για την ταξινόμηση της κίνησης.

Δημιουργία δεδομένων SDN με χρήση mininet: Δημιουργούμε το σύνολο δεδομένων κίνησης SDN χρησιμοποιώντας εξομοιωτή mininet. Τα

υπάρχοντα σύνολα δεδομένων σχεδιάστηκαν για παραδοσιακά δίκτυα και περιλαμβάνουν μόνο ένα μέρος των πληροφοριών που είναι διαθέσιμες στο SDN. (SDN Dataset)

Ταξινόμηση της κυκλοφορίας σε καλοήθη και κακόβουλη με χρήση μηχανικής μάθησης: Αφού δημιουργήσουμε το σύνολο δεδομένων κίνησης SDN, εφαρμόζονται διαφορετικοί αλγόριθμοι Machine Learning για να ταξινομήσει την κυκλοφορία σε καλοήθη και κακόβουλη κατηγορία. Αυτό το εκπαιδευμένο μοντέλο μπορεί επίσης να χρησιμοποιηθεί σε πραγματικό χρόνο.

Ανίχνευση της επίθεσης στον κεντρικό υπολογιστή: Για την ανίχνευση της επίθεσης σε κεντρικούς υπολογιστές, τα αποτελεσματικά χαρακτηριστικά στο σύνολο δεδομένων αναλύονται από το μοντέλο μηχανικής εκμάθησης και ανιχνεύουν τον τύπο της επισκεψιμότητας.

Μοντέλα Μηχανικής Μάθησης ταξινόμησης

Ορισμένα μοντέλα που αποδίδουν καλά στις εργασίες ταξινόμησης

Logistic Regression: Μια ταξινόμηση αλγόριθμος στη Μηχανική Μάθηση που χρησιμοποιεί μια σιγμοειδή συνάρτηση για να ταξινομήσετε την είσοδο σε μία από τις πιθανές κλάσεις. Ο αλγόριθμος χρησιμοποιείται κυρίως στο τομέας κυβερνοασφάλειας για τον χαρακτηρισμό των υποθέσεων ως δόλιων ή μη.

Support Vector Classifier: Ένα όριο ή ένα επίπεδο απόφασης διαχωρίζει την κατηγορία των σημείων δεδομένων οπτικοποιώντας διάφορα σημεία δεδομένων. Ανάλογα με τον αριθμό των σημείων δεδομένων, το επίπεδο απόφασης μπορεί να είναι μια ευθεία γραμμή ή ένα επίπεδο υψηλότερης διάστασης. Τα διανύσματα υποστήριξης είναι τα σημεία που βρίσκονται πιο κοντά στο επίπεδο απόφασης που βοηθούν στον υπολογισμό του περιθωρίου του επιπέδου απόφασης. Ένα επίπεδο απόφασης μεγάλου περιθωρίου είναι προτιμότερο από ένα επίπεδο απόφασης μικρού περιθωρίου. Ο καλύτερος τρόπος διαχωρισμού των διαφορετικών κλάσεων είναι να χρησιμοποιήσετε ένα γενικευμένο επίπεδο απόφασης.

K-Nearest Neighbor: Είναι ένας αλγόριθμος μάθησης χωρίς επίβλεψη που λειτουργεί με βάση την αρχή ότι παρόμοια πράγματα υπάρχουν μαζί. Ο

αλγόριθμος λειτουργεί προβλέποντας την ετικέτα των νέων δεδομένων δοκιμής κατά υπολογισμός της απόστασης μεταξύ των δεδομένων δοκιμής και άλλων γειτόνων δείγματα εκπαίδευσης. Η απόσταση υπολογίζεται χρησιμοποιώντας την Ευκλείδεια απόσταση. Άλλα μέτρα απόστασης μπορούν επίσης να χρησιμοποιειθούν όπως το Manhattan Distance και το Minkowski Distance.

Random Forest: *Δ*ιαφορετικά δέντρα αποφάσεων εκπαιδεύονται στο σύνολο δεδομένων. Βγάζει μια κλάση που είναι η πλειοψηφία των διαφόρων δέντρων αποφάσεων. Ένας μεγάλος αριθμός δέντρων απόφασης χρησιμοποιείται για τα τελικά αποτελέσματα ταξινόμησης.

Artificial Neural Network(ANN): Αποτελείται από πολλά στρώματα α)Επίπεδο εισόδου που αποτελείται από ένα σύνολο νευρώνων εισόδου. β)Στρώμα εξόδου που αποτελείται από ένα σύνολο κλάσεων στις οποίες αντιστοιχίζονται οι νευρώνες εισόδου. γ) Το κρυφό στρώμα αποτελείται από υπολογισμούς για τη λεπτή ρύθμιση των βαρών στο επίπεδο εισόδου για να ελαχιστοποιηθεί το σφάλμα. Οι είσοδοι περνούν στο κρυφό στρώμα. Σε κάθε σύνδεση εκχωρούνται βάρη και κάθε βάρος πολλαπλασιάζεται με νευρώνες εισόδου και προστίθεται προκατάληψη σε αυτά. Η τιμή μεταβιβάζεται στη συνάρτηση ενεργοποίησης για την επιλογή του νευρώνα για εξαγωγή χαρακτηριστικών. Η ίδια διαδικασία ακολουθεί και για άλλα κρυφά επίπεδα και το επίπεδο εξόδου δίνει την πιθανότητα κλάσης ως έξοδο.