**Χαροκόπειο Πανεπιστήμιο Τμήμα Πληροφορικής και Τηλεματικής**

DDoS attack detection in Software-Defined Networking

Νικόλας Μαυρόπουλος it21865

4ο Έτος 8ο Εξάμηνο

Επιβλέπων καθηγητής: Ειρήνη Λιώτου Ημερομηνία: 20/05/2022

**Automated DDOS attack detection in software defined networking**

Το SDN (Software-Defined Networking) είναι ένα παράδειγμα δικτύωσης που επαναπροσδιορίζει τον όρο δίκτυο επιτρέποντας στις συσκευές δικτύου να μπορούν να προγραμματιστούν. Το SDN επιτρέπει στους μηχανικούς δικτύων να παρακολουθούν και να ελέγχουν γρήγορα τα δίκτυά τους από μια κεντρική τοποθεσία, καθώς και να ανακαλύπτουν κακόβουλη κυκλοφορία και αποτυχίες συνδέσεων. Το SDN, παρά την ευελιξία του, είναι ευάλωτο σε επιθέσεις όπως το DDoS, το οποίο μπορεί να φέρει ολόκληρο το δίκτυο σε αδιέξοδο. 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. Ο όγκος επίθεσης DDoS 1,3 TBps διέκοψε τους διακομιστές github στις 28 Φεβρουαρίου 2018. Για να αντιμετωπιστεί αυτή η επίθεση, προτείνεται η χρήση μηχανικής εκμάθησης για τη διάκριση της καλοήθους κυκλοφορίας από την κίνηση επιθέσεων DDoS.

Το SDN έρχεται σε αντίθεση με τη σημερινή αρχιτεκτονική δικτύου, η οποία βασίζεται σε υλικό και ορίζεται από διακόπτες, δρομολογητές και άλλες υποδομές δικτύου. Το επίπεδο δεδομένων είναι το μόνο μέρος του διακόπτη SDN στην κεντρική αρχιτεκτονική SDN, ενώ το επίπεδο ελέγχου μετατοπίζεται σε μια άλλη οντότητα που ονομάζεται ελεγκτής. Εκτός από τα πολυάριθμα οφέλη που προσφέρει το SDN, έχει ελαττώματα ασφαλείας που μπορούν να αξιοποιηθούν σε πολλαπλά αρχιτεκτονικά επίπεδα.

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

2)*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)*Data plane*: Ο εισβολέας μπορεί να επιτεθεί στο επίπεδο δεδομένων πλημμυρίζοντας τον πίνακα ροής του διακόπτη, με αποτέλεσμα μια επίθεση υπερχείλισης του πίνακα ροής.

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:*** Δημιουργoύμε 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.

***Ταξινόμηση της κυκλοφορίας σε καλοήθη και κακόβουλη χρήση Mηχανικής 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.

Ορισμένα μοντέλα που αποδίδουν καλά στις εργασίες ταξινόμησης αναφέρονται παρακάτω.

***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.

***Hybrid Machine learning Model:*** Σε αυτό το μοντέλο, ένα ή περισσότερα μοντέλα μηχανικής μάθησης συνδυάζονται για να ξεπεραστούν τα μειονεκτήματα ενός του άλλου.

Παρακάτω συζητούνται τα σημαντικά χαρακτηριστικά που υπάρχουν στο σύνολο δεδομένων και χρησιμοποιούνται από έναν αλγόριθμο μηχανικής εκμάθησης για την αποτελεσματική ταξινόμηση της κυκλοφορίας.

***Average Packet count per flow (APPF):*** Ένας εισβολέας μπορεί να χρησιμοποιήσει το γεγονός ότι η IP πηγής χρησιμοποιείται ως διαφοροποιητικό στοιχείο για τον προσδιορισμό μιας ροής στο SDN προς όφελός του. Ως αποτέλεσμα, ο εισβολέας να πλημμυρίσει τον πίνακα ροής με διαφορετικές διευθύνσεις IP χρησιμοποιώντας πλαστές διευθύνσεις IP. Ο εισβολέας θέλει απλώς να γεμίσει τον πίνακα ροής με πακέτα δεδομένων και όχι να τα στείλει. Καθώς ο αριθμός των πακέτων που παραδίδονται σε μια επίθεση μειώνεται, το APPF μειώνεται σε μια επίθεση και αυξάνεται σε έναν καλοήθη χρήστη. Αυτή η δυνατότητα μπορεί να χρησιμοποιηθεί για τον εντοπισμό του DDoS επίθεση.

***Average Byte count per flow (ABPF):*** Στο SDN, ο μέσος αριθμός byte ανά ροή μπορεί επίσης να χρησιμοποιηθεί για να υποδείξει μια επίθεση. Το ABPF μειώνεται επίσης σε περίπτωση επίθεσης. Αυτή η δυνατότητα μπορεί επίσης να χρησιμοποιηθεί για εντοπίσει την επίθεση DdoS.

***Total number of flows in a switch:*** Μια ροή είναι η διέλευση πακέτων μεταξύ των κεντρικών υπολογιστών αποστολής και λήψης ενός δικτύου. Στον διακόπτη, διατηρείται ένας πίνακας ροής που περιέχει όλες τις λεπτομέρειες ροής τοπολογιών. Σε περίπτωση επίθεσης, ο διακόπτης που είναι συνδεδεμένος με τον κεντρικό υπολογιστή-στόχο βρέθηκε ότι περιέχει τον μέγιστο αριθμό εισαγωγών ροής. Η περιοδική παρακολούθηση των κεντρικών υπολογιστών δείχνει ότι ο διακόπτης στόχος έχει μέγιστο αριθμό εισαγωγών ροής. Επομένως, ο αριθμός των καταχωρήσεων ροής είναι ένα σημαντικό χαρακτηριστικό για την ταξινόμηση της κίνησης ως καλοήθους ή κακόβουλης.

***Protocol:*** Οποιαδήποτε απόκλιση από το τυπικό πρωτόκολλο κυκλοφορίας μπορεί να βοηθήσει στον εντοπισμό της επίθεσης.

***Duration:*** Η διάρκεια απεικονίζει τη διάρκεια εισόδου της ροής, στη ροή πίνακας ενός διακόπτη. Η κυκλοφορία επιθέσεων παραμένει για μεγαλύτερη διάρκεια σε σύγκριση με την κανονική κυκλοφορία. Έτσι, η διάρκεια κατά την οποία μια ροή παραμένει ενεργή στο διακόπτη παίζει σημαντικό παράγοντα για τον προσδιορισμό του κακόβουλου κεντρικού υπολογιστή. Η διάρκεια έχει υψηλή αξία σε περίπτωση επίθεσης σε σύγκριση με την καλοήθη κυκλοφορία.

***Number of Packet\_in messages:*** Τα μηνύματα Packet\_in δημιουργούνται από τους κεντρικούς υπολογιστές και αποστέλλονται στον ελεγκτή όταν δεν έχει αντίστοιχη περιγραφή ροής στον πίνακα ροής. Σε απόκριση, ο ελεγκτής στέλνει το μήνυμα Packet\_Out. Όταν οι εισβολείς χρησιμοποίησαν πλαστές διευθύνσεις IP, ένας μεγάλος αριθμός μηνυμάτων Packet\_in αναφέρονται στον ελεγκτή. Όταν το μήνυμα Packet\_in δημιουργείται από το διακόπτη είναι γνωστό ως συμβάν. Οι χειριστές συμβάντων συσχετίζονται με κάθε συμβάν που δημιουργείται. Έτσι, για να λάβετε τον αριθμό των μηνυμάτων Packet\_in που δημιουργούνται, ένας μετρητής ενημερώνεται στη ρουτίνα χειρισμού συμβάντων μηνυμάτων Packet\_in. Ο αριθμός των μηνυμάτων Packet\_in αυξάνεται σε περίπτωση επίθεσης.

***Packet rate:*** Ο ρυθμός πακέτων ορίζεται ως ο αριθμός των πακέτων που αποστέλλονται ανά δευτερόλεπτο. Τόσο η καλοήθης όσο και η κακόβουλη κυκλοφορία στέλνουν 450 πακέτα ανά δευτερόλεπτο, αλλά επειδή ο εισβολέας χρησιμοποιεί πλαστές διευθύνσεις IP, τα ποσοστά πακέτων αναφέρθηκαν ότι είναι χαμηλότερα.

***Port Bandwidth:*** Το εύρος ζώνης θύρας ορίζεται ως το άθροισμα των ληφθέντων byte και των μεταδιδόμενων byte. Τα στοιχεία συλλέγονται ως στατιστικά στοιχεία θύρας από το διακόπτη περιοδικά σε τακτά χρονικά διαστήματα. Καθώς ο εισβολέας στέλνει περισσότερα αιτήματα και λιγότερα δεδομένα, το εύρος ζώνης θύρας είναι μικρότερο, γεγονός που υποδεικνύει την επίθεση.

**FADM: DDoS Flooding Attack Detection and**

**Mitigation System in Software-Defined Networking**

Προτείνουμε το FADM, ένα αποτελεσματικό και ελαφρύ πλαίσιο για τον εντοπισμό και τον μετριασμό των επιθέσεων DDoS στο SDN. Αρχικά, συλλέγονται οι πληροφορίες κίνησης δικτύου μέσω του ελεγκτή SDN και των πρακτόρων sFlow. Στη συνέχεια, μια εντροπία μέθοδος χρησιμοποιείται για τη μέτρηση των χαρακτηριστικών του δικτύου και ο ταξινομητής του SVM εφαρμόζεται για τον εντοπισμό ανωμαλιών δικτύου. Για να κρατήσει το κύριο δίκτυο λειτουργώντας κανονικά, προτείνουμε έναν αποτελεσματικό μηχανισμό μετριασμού των επιθέσεων που βασίζεται στη λίστα λευκών και στη μετεγκατάσταση επισκεψιμότητας. Με την εισαγωγή του παράγοντα μετριασμού στο δίκτυο, η κυκλοφορία επιθέσεων μπορεί να αποκλειστεί έγκαιρα, ενώ η καλοήθης κυκλοφορία μπορεί να προωθηθεί ως συνήθως.

Για να αποφευχθεί η διακοπή της επικοινωνίας των νόμιμων χρηστών, δεν μπορούμε απλά να αποχωρήσουμε όλη την κίνηση επιθέσεων, επομένως εισάγουμε τον παράγοντα μετριασμού στο δίκτυο. Όταν συμβαίνει μια επίθεση DDoS, όλες οι ύποπτες ροές κυκλοφορίας επιθέσεων μετεγκαθίστανται στον πράκτορα μέσω των εγκατεστημένων κανόνων ροής μπαλαντέρ. Ωστόσο, ορισμένες καλοήθεις ροές κυκλοφορίας μπορεί επίσης να μετεγκατασταθεί και στον παράγοντα μετριασμού, επομένως πρέπει να υπάρχει τρόπος να τα αναγνωρίσετε και να εγκαταστήσετε επιπλέον κανόνες προώθησης.

Οι κύριες συνεισφορές μπορούν να συνοψιστούν ως ακολουθεί:

1) Προτείνουμε ένα σχήμα ανίχνευσης επιθέσεων DDoS σε πραγματικό χρόνο, το οποίο μπορεί να βελτιώσει αποτελεσματικά την επικαιρότητα και την ακρίβεια της ανίχνευσης επιθέσεων υιοθετώντας τις μεθόδους συλλογής πληροφοριών βάσει ελεγκτών και sFlow, τη μέθοδο εξαγωγής χαρακτηριστικών βάσει εντροπίας και τη μέθοδο ταξινόμησης βάσει SVM.

2) Προτείνουμε έναν αποτελεσματικό μηχανισμό μετριασμού επιθέσεων DDoS που βασίζεται στη λευκή λίστα και στη δυναμική ενημέρωση των κανόνων προώθησης. Με την εισαγωγή του παράγοντα μετριασμού στο δίκτυο, η κυκλοφορία επιθέσεων μπορεί να αποκλειστεί έγκαιρα, ενώ η καλοήθης κυκλοφορία προωθείται ως συνήθως, γεγονός που εμποδίζει την εξάντληση των πόρων του ελεγκτή και διασφαλίζει ότι οι νόμιμοι χρήστες μπορούν να έχουν κανονική πρόσβαση στο δίκτυο.

3) Εφαρμόζουμε ένα αποτελεσματικό, ελαφρύ και ανεξάρτητο από το πρωτόκολλο πρωτότυπο σύστημα που ονομάζεται FADM. Μπορεί να ανιχνεύσει με ακρίβεια πολλαπλές επιθέσεις πλημμύρας DdoS και επιτρέπει στο δίκτυο να ανακάμψει γρήγορα.

**Αρχές Σχεδιασμού:** Πρώτον, το σύστημα θα πρέπει να είναι ακριβές και ευαίσθητο σε επιθέσεις πλημμύρας DDoS για να εγγυάται την ανίχνευση σε πραγματικό χρόνο. Επιπλέον, οι επιθέσεις θα πρέπει να μετριάζονται αποτελεσματικά για να διατηρηθεί το δίκτυο ισχυρό. Τέλος, προσπαθούμε να επιτύχουμε τους στόχους που αναφέρθηκαν παραπάνω με το όλο σύστημα να είναι όσο το δυνατόν πιο ελαφρύ και κλιμακωτό.

**Αρχιτεκτονική του συστήματος:** Η αρχιτεκτονική του FADM αποτελείται από δύο κύριες ενότητες 1) Μονάδα ανίχνευσης DDoS και 2) DDoS μονάδα μετριασμού.

1) Μονάδα ανίχνευσης DdoS: Ο στόχος είναι η ανίχνευση επιθέσεων DDoS σε πραγματικό χρόνο. Αυτή η λειτουργική μονάδα εκτελείται ως εφαρμογή στον ελεγκτή, ο οποίος είναι υπεύθυνος για τη συλλογή πληροφοριών κίνησης, την εξαγωγή λειτουργιών δικτύου και τον αυτόματο εντοπισμό ανωμαλιών δικτύου.

2) Ενότητα μετριασμού DdoS: Ο σκοπός αυτής της ενότητας είναι να μετριάσει αποτελεσματικά τις επιθέσεις DDoS για να επιτρέψει στο δίκτυο να ανακάμψει γρήγορα. Αυτή η ενότητα αποτελείται από δύο στοιχεία, Διακομιστής Μετριασμού και Πράκτορας Μετριασμού. Ο διακομιστής μετριασμού εκτελείται ως εφαρμογή στον ελεγκτή, ενώ ο πράκτορας μετριασμού εκτελείται σε έναν κεντρικό υπολογιστή στο δίκτυο SDN.

***Μονάδα ανίχνευσης DdoS:*** Χωρίζεται σε τρεις φάσεις: 1) συλλογή πληροφοριών, 2) εξαγωγή χαρακτηριστικών και 3) ανίχνευση επίθεσης.

1) Συλλογή πληροφοριών: Στο περιβάλλον SDN, υπάρχουν δύο μέθοδοι που χρησιμοποιούνται για τη συλλογή πληροφοριών. Το πρώτο βασίζεται στο πρωτόκολλο OF. Σε αυτή τη μέθοδο, ο ελεγκτής στέλνει περιοδικά ένα μήνυμα αίτησης κατάστασης στους διακόπτες και οι διακόπτες απαντούν με ένα ή περισσότερα μηνύματα απάντησης που περιέχουν στατιστικά στοιχεία ροής. Αυτή η μέθοδος μπορεί να συγκεντρώσει τη συνολική κίνηση που διέρχεται από το διακόπτη με πλήρη λεπτομέρεια. Ωστόσο, όταν το δίκτυο υφίσταται επίθεση DDoS υψηλού ποσοστού, το εύρος ζώνης μεταξύ του ελεγκτή και των διακοπτών εξαντλείται από την κίνηση επιθέσεων, ο πίνακας ροής του διακόπτη είναι γεμάτος και τα μεγέθη των απαντήσεων είναι πολύ μεγάλα. Τέλος, ο ελεγκτής δεν μπορεί να λάβει έγκαιρα τα μηνύματα απάντησης ή η σύνδεση μεταξύ του διακόπτη έχει διακοπεί.

Η δεύτερη μέθοδος βασίζεται σε μηχανισμό παρακολούθησης ροής χρησιμοποιώντας δείγματα πακέτων. Το sFlow-RT είναι ένα λογισμικό παρακολούθησης της κυκλοφορίας που μπορεί να χρησιμοποιηθεί σε δίκτυα SDN. Στο sFlow-RT, τα δείγματα ροής και τα δείγματα μετρητή συλλέγονται από sFlow Agents ενσωματωμένα σε συσκευές δικτύου και αποστέλλονται περιοδικά στο sFlow Collector. Αυτή η μέθοδος δεν καταναλώνει το εύρος ζώνης μεταξύ του ελεγκτή και των διακοπτών, επομένως μπορεί να ξεπεράσει τα εμπόδια που παρουσιάζονται στην πρώτη μέθοδο. Ωστόσο, λόγω της περιοδικής δειγματοληψίας πακέτων από το sFlow, δεν μπορεί να συλλέξει τις πληροφορίες όλων των πακέτων, κάτι που θα έχει κάποιο αντίκτυπο στην ακρίβεια του εντοπισμού ανωμαλιών.

Για την αντιμετώπιση των προβλημάτων των δύο μεθόδων που αναφέρονται παραπάνω, προτείνουμε μια μέθοδο συλλογής πληροφοριών απευθείας μέσω του ελεγκτή SDN. Σύμφωνα με το πρωτόκολλο του OF, εάν δεν υπάρχει αντίστοιχη καταχώρηση ροής κατά την άφιξη ενός πακέτου, ο μεταγωγέας θα στείλει ένα μήνυμα Packet-In που περιέχει την κεφαλίδα του πακέτου στον ελεγκτή για ενέργειες. Δεδομένου ότι κάθε νέα ροή κυκλοφορίας θα στέλνει ένα μήνυμα Packet-In στον ελεγκτή, μπορούμε να συλλέξουμε όλες τις πληροφορίες κυκλοφορίας ολόκληρου του δικτύου απευθείας μέσω του ελεγκτή, το οποίο δεν δημιουργεί καμία πρόσθετη επικοινωνία. Από την άλλη πλευρά, όταν η κανονική κίνηση φτάσει σε υψηλό ρυθμό, τα buffer μεταγωγών θα εξαντληθούν από την κανονική κυκλοφορία και κάποια κίνηση επίθεσης θα απορριφθεί, με αποτέλεσμα η μέθοδος που βασίζεται σε Controller-based (CT-based) να μην μπορεί να συλλέξει πλήρως τις πληροφορίες. Αλλά ο sFlow Collector μπορεί να λάβει τα πακέτα δειγματοληψίας κανονικά. Επομένως, προκειμένου να βελτιωθεί η ακρίβεια της συλλογής πληροφοριών, στο Μικρό Γραφείο / Σπίτι Περιβάλλοντα γραφείου, ο κανονικός ρυθμός επισκεψιμότητας είναι χαμηλός, η μέθοδος που βασίζεται σε CT χρησιμοποιείται για τη συλλογή πληροφοριών. Ενώ σε περιβάλλοντα μεγαλύτερων επιχειρήσεων ή ISP, χρησιμοποιούμε τη μέθοδο που βασίζεται σε sFlow.

2) Εξαγωγή χαρακτηριστικών: Σκοπός του είναι να εξάγει το τρέχοντα χαρακτηριστικά δικτύου από τις συλλεγόμενες πληροφορίες. Όταν ξεκινά μια επίθεση DDoS, ένας μεγάλος αριθμός κατανεμημένων κακόβουλων τελικών σημείων επιτίθεται ταυτόχρονα σε έναν συγκεκριμένο στόχο, γεγονός που προκαλεί την αλλαγή της κατανομής των διευθύνσεων IP και των θυρών εντός του δικτύου. Η εντροπία είναι ένα μέτρο της αβεβαιότητας των τυχαίων μεταβλητών στη θεωρία της πληροφορίας. Οι υψηλές τιμές εντροπίας δηλώνουν μια πιο διασπαρμένη κατανομή πιθανοτήτων, ενώ οι χαμηλές τιμές εντροπίας δηλώνουν τη συγκέντρωση μιας κατανομής. Επομένως, χρησιμοποιούμε την εντροπία για να μετρήσουμε τις αλλαγές των χαρακτηριστικών του δικτύου.

3) Ανίχνευση επίθεσης: Η ανίχνευση επιθέσεων DDoS μπορεί να θεωρηθεί ως ένα πρόβλημα δυαδικής ταξινόμησης στον τομέα της μηχανικής μάθησης, το οποίο ταξινομεί την τρέχουσα κατάσταση δικτύου ως κανονική ή μη κανονική. Ο ταξινομητής SVM είναι ένας δυαδικός αλγόριθμος ταξινόμησης που βασίζεται στη θεωρία στατιστικής μάθησης και στη θεωρία ελαχιστοποίησης δομικών κινδύνων. Χρησιμοποιώντας αυτή τη μέθοδο, μπορούμε να εντοπίσουμε με ακρίβεια επιθέσεις DDoS σε πραγματικό χρόνο.

***Ενότητα μετριασμού DdoS:*** Χωρίζεται σε τρεις κύριες λειτουργίες

1) Διαδικασία εργασίας: Αυτή η ενότητα περιλαμβάνει δύο στοιχεία: διακομιστή μετριασμού και παράγοντα μετριασμού. Η διαδικασία εργασίας αυτής της ενότητας χωρίζεται σε πέντε βήματα: i) Όταν ανιχνεύεται μια επίθεση DDoS από τη μονάδα ανίχνευσης, η μονάδα μετριασμού εισέρχεται στην κατάσταση μετριασμού επίθεσης, ii) Στη συνέχεια, ο διακομιστής μετριασμού προσδιορίζει την κίνηση επιθέσεων και εγκαθιστά έναν κανόνα ροής μετεγκατάστασης που έχει όλα τα πεδία μπαλαντέρ εκτός από το πρωτόκολλο δικτύου, τις διευθύνσεις MAC και IP προορισμού, iii) Όλες οι ροές κυκλοφορίας που ταιριάζουν με τον κανόνα ροής χαρακτήρων μπαλαντέρ μετεγκαθίστανται στον παράγοντα μετριασμού, συμπεριλαμβανομένης της παρόμοιας κίνησης επιθέσεων και κάποιας καλοήθης κυκλοφορίας, iv) Η καλοήθης κίνηση προσδιορίζεται από τον παράγοντα μετριασμού και θα προωθηθεί στον διακομιστή μετριασμού, ενώ η άλλη κίνηση απορρίπτεται απευθείας, v) Ο διακομιστής μετριασμού εγκαθιστά έναν κανόνα ροής προώθησης για την καλοήθη κίνηση και τον προωθεί στον κεντρικό υπολογιστή-στόχο.

Παρακάτω, παρουσιάζουμε τη λεπτομερή υλοποίηση των τριών βασικών λειτουργιών

2) Συλλογή λευκής λίστας: Υπάρχουν δύο τύποι λευκών λιστών, το ένα είναι η στατική λευκή λίστα που έχει οριστεί από τον διαχειριστή του δικτύου και το άλλο είναι η δυναμική λευκή λίστα. Εάν το τρέχον δίκτυο βρίσκεται σε κανονική κατάσταση, ο διακομιστής μετριασμού αποθηκεύει τις πληροφορίες ροής κυκλοφορίας που συλλέγονται από τη μονάδα εντοπισμού σε μια βάση δεδομένων, συμπεριλαμβανομένων των πληροφοριών χρόνου συλλογής. Σε περιοδικά διαστήματα, ο διακομιστής αναλύει τις αποθηκευμένες πληροφορίες για ενημέρωση της λευκής λίστας σύμφωνα με τους ακόλουθους κανόνες:

* Η ροή έχει μια ροή ζεύγους
* Ο αριθμός των ροών με την ίδια διεύθυνση IP προέλευσης υπερβαίνει την τιμή κατωφλίου
* Ο αριθμός των ημερών που η ίδια διεύθυνση IP προέλευσης εμφανίζεται στη βάση δεδομένων υπερβαίνει την τιμή κατωφλίου

Οι διευθύνσεις IP προέλευσης που πληρούν τους παραπάνω κανόνες προστίθενται στη λευκή λίστα και αποστέλλονται στον παράγοντα μετριασμού ταυτόχρονα. Οι τιμές κατωφλίου πρέπει να οριστούν σύμφωνα με την κλίμακα του δικτύου.

3) Μεταναστευτική κίνηση επιθέσεων: Όταν το δίκτυο υποφέρει από επιθέσεις DDoS, η κίνηση επίθεσης πρέπει να μετεγκατασταθεί ή να απορριφθεί για να αποφευχθεί η εξάντληση των πόρων και του εύρους ζώνης του ελεγκτή. Λόγω του περιορισμένου μεγέθους του πίνακα ροής διακόπτη, δεν είναι δυνατή η εγκατάσταση κανόνων ροής μετεγκατάστασης ή απόρριψης για κάθε κίνηση επίθεσης, επομένως μπορούμε να εγκαταστήσουμε μόνο έναν κανόνα ροής μπαλαντέρ. Όλες οι ύποπτες ροές κυκλοφορίας επιθέσεων μεταφέρονται πρώτα στον παράγοντα μετριασμού και στη συνέχεια προσδιορίζονται περαιτέρω από αυτόν.

Εάν η κίνηση είναι καλοήθης κίνηση, προωθείται στον διακομιστή μετριασμού για να εγκαταστήσει έναν κανόνα ροής προώθησης. Εάν η διεύθυνση IP προέλευσης βρίσκεται στη λευκή λίστα, η επισκεψιμότητα αναγνωρίζεται ως καλοήθης κίνηση και αντιμετωπίζεται από τον ελεγκτή κανονικά. Εάν η διεύθυνση IP προέλευσης δεν βρίσκεται στη λευκή λίστα και η διεύθυνση IP προορισμού βρίσκεται στη λίστα προστατευμένου κεντρικού υπολογιστή, η κίνηση προσδιορίζεται ως επίθεση για τον προστατευμένο κεντρικό υπολογιστή-στόχο. Στη συνέχεια, ο διακομιστής μετριασμού δημιουργεί έναν χαρακτήρα μπαλαντέρ κανόνας ροής για την κίνηση επίθεσης.

4) Προώθηση καλοήθους κυκλοφορίας: Αφού εγκατασταθεί ο κανόνας ροής μετεγκατάστασης στον μεταγωγέα, εάν η ευνοϊκή κυκλοφορία έχει το ίδιο πρωτόκολλο δικτύου και διευθύνσεις προορισμού με την κίνηση επίθεσης θα ταιριάζει επίσης με τον κανόνα ροής μετεγκατάστασης και θα μεταφερθεί στον παράγοντα μετριασμού. Για να αποτραπεί η απόρριψη αυτής της καλοήθους επισκεψιμότητας, πρέπει να προωθηθεί στον κεντρικό υπολογιστή προορισμού μέσω του διακομιστή μετριασμού και του παράγοντα που συνεργάζονται. Ο παράγοντας μετριασμού συλλαμβάνει όλα τα πακέτα που έχουν μετεγκατασταθεί και προσδιορίζει την καλοήθη κίνηση από αυτά σύμφωνα με τη λευκή λίστα που λαμβάνεται από τον διακομιστή μετριασμού. Αφού ο διακομιστής μετριασμού λάβει αυτήν την κίνηση, δημιουργεί έναν κανόνα κανονικής ροής προώθησης και ορίζει την ενέργεια για έξοδο στον κεντρικό υπολογιστή προορισμού.

**Συμπεράσματα**

Το Software-Defined Networking (SDN) είναι η αρχιτεκτονική δικτύωσης που ορίζεται από το λογισμικό. Η κίνηση δικτύου ελέγχεται σε ένα κεντρικό τρόπο από τον ελεγκτή που κατευθύνει εξ αποστάσεως την κίνηση μεταξύ των κεντρικών υπολογιστών. Εκτός από έναν τόσο ευέλικτο έλεγχο του δικτύου διαχείρισης της κυκλοφορίας, το δίκτυο εξακολουθεί να είναι επιρρεπές σε διάφορες επιθέσεις. Έτσι, χρησιμοποιούμε τεχνικές μηχανικής μάθησης και FADM, ένα αποτελεσματικό και ελαφρύ πλαίσιο για τον εντοπισμό και τον μετριασμό των επιθέσεων πλημμύρας DDoS σε περιβάλλον SDN, για τη δημιουργία ενός συνόλου δεδομένων SDN και την ταξινόμηση της καλοήθους επισκεψιμότητας από επιθέσεις DDOS. Τα μοντέλα μηχανικής εκμάθησης εκπαιδεύονται στο σύνολο δεδομένων SDN, το οποίο είναι χτισμένο σε έναν εξομοιωτή mininet για να μιμείται ένα σενάριο σε πραγματικό χρόνο, έτσι ώστε το μοντέλο ταξινόμησης να μπορεί να χρησιμοποιηθεί σε πραγματικό χρόνο για να κατηγοριοποιήσει την επισκεψιμότητα βάσει μαθησιακών χαρακτηριστικών. Προτείναμε ένα υβριδικό μοντέλο Support Vector Classifier και Random Forest που ταξινομεί την κυκλοφορία χρησιμοποιώντας αποτελέσματα SVC που στη συνέχεια φιλτράρονται από το Random Forest. Πολλαπλές επιθέσεις πλημμύρας DDoS μπορούν να εντοπιστούν σωστά και να μετριαστούν αποτελεσματικά από το FADM, επιτρέποντας στο δίκτυο να ανακάμψει γρήγορα. Επιπλέον, το FADM έχει χαμηλό γενικό κόστος.

**Βιβλιογραφία**

1. Automated DDOS attack detection in software defined networking (Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay, Neeraj Kumar)

2. FADM DDoS Flooding Attack Detection and Mitigation System in Software Defined Networking (Dingwen Hu, Peilin Hong, Yixin Chen)