Α.Τ.Ε.Ι. ΚΑΛΑΜΑΤΑΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΕΧΝΙΚΕΣ ΑΝΩΝΥΜΟΠΟΙΗΣΗΣ ΣΤΗ ΔΡΟΜΟΛΟΓΗΣΗ ΠΑΚΕΤΩΝ

*Επιβλέπων Καθηγητής:*Πικραμμένος Ιωάννης

Φοιτήτρια: Γεωργαλλή Δέσποινα *ΑΜ: 2009047*

Σπάρτη, Νοέμβριος 2013

Copyright © Δέσποινα Γ. Γεωργαλλή, 2013

Με επιφύλαξη παντός δικαιώματος. Allrightsreserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Α.Τ.Ε.Ι. Καλαμάτας.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ	ΥΠΟΓΡΑΦΕΣ
1.	
2.	
3.	

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Α.Τ.Ε.Ι. Καλαμάτας.

Η συγγραφέας,

Γεωργαλλή Δέσποινα

Περιεχόμενα

Περίληψη 12
Εισαγωγή 13
Κεφάλαιο 1: Σύστημα ανίχνευσης και πρόληψης εισβολών 16
1.1 Εισαγωγή 16
1.2. Σύστημα ανίχνευσης εισβολών 17
1.2.1. Τι προσφέρουν τα IDS 18
1.2.2. Πλεονεκτήματα των IDS 20
1.2.3. Μειονεκτήματα των IDS 20
1.3. Σύστημα πρόληψης εισβολής 21
1.3.1. Τι προσφέρουν τα IPS 22
1.3.2. Πλεονεκτήματα των IPS 23
1.3.3. Μειονεκτήματα των IPS 23
1.4. Διαφορά μεταξύ IDS και IPS συστήματα 24
ΚΕΦΑΛΑΙΟ 2: Συστήματα ανίχνευσης εισβολών 26
2.1 Ορισμός IDS 26
2.1.1. Το IDS προβλέπει τα εξής: 27
2.1.2. Χαρακτηριστικά των συστημάτων ανίχνευσης εισβολών 27
2.1.3. Πλεονεκτήματα και μειονεκτήματα IDS 28
2.1.4. Βασικοί τύποι του συστήματος IDS 28
2.1.5. Ψευδώς θετικά και αρνητικά των IDS 32
2.1.6. Περιορισμοί IDS 32
2.1.7. Σύστημα ανίχνευσης εισβολών εναντίον Firewalls 33
2.1.8. Κορυφαία συστήματα ανίχνευσης εισβολών 34
2.2. Εισαγωγή στο Snort 34
2.2.1. Τι είναι το Snort 35
2.2.2. Αρχιτεκτονική Snort 37
2.2.3. Κανόνες Snort 42
2.2.4. Η τυπική επεξεργασία κανόνων στο Snort 45
2.2.5. Διαδικασία ανίχνευσης του Snort 46
2.3. Εισαγωγή στο Bro 48
2.3.1. Τι είναι το Bro 48
2.3.2. Στόχος σχεδιασμού Bro 49
2.3.3. Αρχιτεκτονική του Bro 50

2.3.4. Χαρακτηριστικά των NIDS Bro ... 52
2.4. Σύγκριση του Bro και του Snort IDS ... 53
ΚΕΦΑΛΑΙΟ 3: Συστήματα πρόληψης εισβολών ... 54
3.1. Ορισμός IPS ... 54
3.1.1. Πλεονεκτήματα των IPS ... 56
3.1.2. Βασικοί τύποι συστήματος IPS ... 57
3.1.3. Ψευδώς θετικά και αρνητικά των IPS ... 61
3.1.4. Σύστημα πρόληψης εισβολών εναντίον firewalls ... 62
3.1.5. Κορυφαία συστήματα IPS ... 62
3.2. Εισαγωγή στο Ossec ... 63
3.2.1. Τι είναι το Ossec ... 64
3.2.2. Δυνατότητες Ossec ... 65
3.2.3. Αρχιτεκτονική Ossec ... 67
3.2.4. Υποστηριζόμενες πλατφόρμες ... 70
3.2.5. Κανόνες Ossec ... 71
3.3. Εισαγωγή στο Suricata ... 74
3.3.1. Τι είναι το Suricata ... 75
3.3.2. Δυνατότητες Suricata ... 76
3.3.3. Πλεονεκτήματα Suricata ... 77
3.3.4. Σύστημα Suricata ... 77
3.3.5. Υποστηριζόμενες πλατφόρμες ... 79
Κεφάλαιο 4: Υβριδικά συστήματα ανίχνευσης και πρόληψης ... 80
4.1. Υβριδικό σύστημα ... 80
4.1.1. Υβριδική λειτουργία ... 82
4.1.2. Πλεονεκτήματα και μειονεκτήματα Hybrid ... 84
4.1.3. Υβριδική αρχιτεκτονική συστήματος ... 84
4.1.4. Προτεινόμενη υβριδική αρχιτεκτονική ... 86
4.1.5. Κίνητρα για υβριδική προσέγγιση ... 87
4.1.6. Υβριδικό μοντέλο που χρησιμοποιεί Snort ... 88
4.1.7. Υβριδική σάρωση ... 90
4.1.8. Υβριδικά Firewalls ... 91
4.2. Αρχιτεκτονική υβριδικού IDS ... 91
4.2.1. Μοναδικά χαρακτηριστικά των υβριδικών IDS ... 94
4.3. Σχεδιασμός NIDS και HIDS υβριδικής ανίχνευσης εισβολής ... 95

4.3.1. Υβριδικό IDS: H-Snort 97
Κεφάλαιο 5: Σύγκριση και υλοποίηση ανίχνευσης και πρόληψης εισβολών 98
5.1. Εισαγωγή 98
5.2. Καθορισμός της ανωνυμίας 100
5.3. Τεχνικές ανωνυμίας 100
5.3.1. Η αντίληψη των Mix 101
5.3.2. Μετρήσεις ανωνυμίας 102
5.4. Μοντέλο 104
5.5. Μοντέλο επίθεσης 105
5.6. Πληροφορίες θεωρητικών ανωνυμιών μετρήσεων 106
Βιβλιογραφία 110
Δημοσιεύσεις 110
Τεχνικές Αναφορές 111
Βιβλία 111
Ιστοσελίδες 111

Περιεχόμενα εικόνων

Εικόνα 1: Διαφορές μεταξύ IDS και IPS....25

Εικόνα 2: Λειτουργία IDS....27

Εικόνα 3: Αρχιτεκτονική Snort....37

Εικόνα 4: Αρχιτεκτονική Bro....51

Εικόνα 5: Λειτουργία IPS....56

Εικόνα 6: Στοιχεία Ossec....65

Εικόνα 7: Αρχιτεκτονική Ossec....68

Εικόνα 8: Αρχιτεκτονική Ossec....69

Εικόνα 9: Κανόνες Ossec....72

Εικόνα 10: Σύστημα Suricata....78

Εικόνα 11: Υβριδική λειτουργία....84

Εικόνα 12: Διαπίστωση ανωμαλίας κατά την πρώτη κατάχρηση μετά την ανίχνευση....85

Εικόνα 13: Παράλληλη προσέγγιση....85

Εικόνα 14: Ανίχνευση κατάχρησης αρχικά μετά ανίχνευση ανωμαλιών....86

Εικόνα 15 : Υβριδική προσέγγιση....88

Εικόνα 16: Υβριδικό μοντέλο με χρήση Snort....89

Εικόνα 17: Αρχιτεκτονική υβριδικού IDS....93

Εικόνα 18: Σχεδίαση υβριδικών NIDS και HIDS....96

Εικόνα 19: Πρότυπο για σύστημα ανωνυμίας....104

Εικόνα 20: Τοποθέτηση ανωνυμιών....107

Περίληψη

Στην σημερινή εποχή οι άνθρωποι και οι επιχειρήσεις επιδιώκουν την προστασία των πληροφοριών και της ιδιοκτησίας από επιθέσεις εισβολών οι οποίοι μπορούν να κλέψουν, δωροδοκήσουν, αλλοιώσουν ή καταστρέψουν, επιτρέποντας παράλληλα οι πληροφορίες αυτές και οι αντίστοιχες ιδιοκτησίες, να είναι προσιτές και προσβάσιμες σε συγκεκριμένους-εξουσιοδοτημένους χρήστες. Επειδή, όλο και περισσότερο αναπτύσσονται νέες επιθέσεις εισβολών υπήρξε η ανάγκη δημιουργίας συστημάτων τα οποία θα εντόπιζαν και θα εμπόδιζαν την νέα επίθεση. Συνεπώς, δημιουργήθηκαν συστήματα τα οποία ανιχνεύουν και αποτρέπουν τις επιθέσεις εισβολών να αλλοιώνουν ή να καταστρέφουν πληροφορίες στις οποίες δεν έχουν πρόσβαση.

Στα πλαίσια της πτυχιακή αυτής εργασίας γίνεται προσπάθεια για την καταγραφή των συστημάτων ανίχνευσης και πρόληψης εισβολών και πως μπορούν να αντιμετωπιστούν.

Στο πρώτο κεφάλαιο περιγράφονται οι έννοιες ανίχνευσης και πρόληψης εισβολών και τι προσφέρουν αντίστοιχα. Ακόμη, γίνεται μια αναφορά στις διαφορές μεταξύ των δυο συστημάτων.

Στο δεύτερο κεφάλαιο γίνεται αναφορά στα χαρακτηριστικά ανίχνευσης και προσπάθεια ανάλυσης των δυο βασικότερων συστημάτων ανίχνευσης, Snort και Bro. Συγκεκριμένα, αναλύεται η λειτουργία τους και η αρχιτεκτονική τους.

Στο τρίτο κεφάλαιο γίνεται αναφορά στα χαρακτηριστικά πρόληψης και προσπάθεια ανάλυσης των δυο βασικότερων συστημάτων πρόληψης, Suricata και Ossec. Συγκεκριμένα, αναλύεται η λειτουργία τους και η αρχιτεκτονική τους.

Στο τέταρτο κεφάλαιο γίνεται μια προσπάθεια ανάλυσης υβριδικού μοντέλου. Συγκεκριμένα, αναλύεται η λειτουργία και χαρακτηριστικά ενός υβριδικού.

Στον πέμπτο κεφάλαιο γίνεται προσπάθεια αναφοράς σύγκρισης και υλοποίησης ανίχνευσης και πρόληψης εισβολών.

Εισαγωγή

Στην παρούσα πτυχιακή εργασία θα αναφερθούμε πως μπορούμε να προστατέψουμε την μεταφορά πληροφοριών από υπολογιστή σε υπολογιστή από γνωστές και άγνωστες επιθέσεις εισβολών. Υπάρχουν δυο συστήματα τα οποία μπορούν να προστατέψουν τις πληροφορίες από τις επιθέσεις, τα οποία είναι η ανίχνευση εισβολών και η πρόληψη εισβολών.

Το σύστημα ανίχνευσης μπορεί να εντοπίζει τις επιθέσεις οι οποίες γίνονται κατά την μεταφορά των πληροφοριών οποιαδήποτε στιγμή, το οποίο εμείς δεν μπορούμε να το αντιληφθούμε. Το σύστημα ανίχνευσης αναγνωρίζει τις ενέργειες οι οποίες γίνονται πριν πραγματοποιηθεί η επίθεση. Υπάρχουν πολλά συστήματα ανίχνευσης εισβολών τα οποία μπορούμε να εγκαταστήσουμε σε ένα υπολογιστή, όμως τα πιο κορυφαία είναι το Snort και το Bro. Το σύστημα Snort έχει την δυνατότητα να αναλύει την δικτυακή κίνηση σε πραγματικό χρόνο. Επίσης ειδοποιεί για πιθανές επιθέσεις, μπλοκάρει και καταγράφει πακέτα σε δίκτυα. Χρησιμοποιεί ένα συνδυασμό μηχανισμών ανάλυσης των πρωτοκόλλων επικοινωνίας και αναγνώρισης προτύπων με στόχο να ανιχνεύει ανωμαλίες και επιθέσεις. Το σύστημα Bro παρακολουθεί παθητικά την κυκλοφορία του δικτύου και ψάχνει για ύποπτη δραστηριότητα. Το σύστημα Bro έχει την δυνατότητα να ανιχνεύει εισβολείς απ την πρώτη κυκλοφορία του δικτύου ανάλυσης.

Το σύστημα πρόληψης μπορεί να αποτρέπει επιθέσεις τις οποίες δεν μπόρεσε να σταματήσει κάποιο antivirus. Το σύστημα πρόληψης παρακολουθεί τις επιθέσεις ώστε να τις προσδιορίσει, να καταγράψει πληροφορίες σχετικά για τις επιθέσεις και να προσπαθήσει να τις εμποδίσει ή να τις σταματήσει. Υπάρχουν πολλά συστήματα πρόληψης τα οποία μπορούμε να εγκαταστήσουμε στον υπολογιστή, όμως τα πιο κορυφαία είναι το Ossec και το Suricata. Το σύστημα Ossec μπορεί να εγκατασταθεί ως αυτόνομο εργαλείο και να παρακολουθήσει μια υποδοχή. Το σύστημα Suricata στηρίζεται στον κινητήρα που χρησιμοποιείται εξωτερικά ώστε να αναπτυχθούν κανόνες που ορίζουν την παρακολούθηση της κίνησης.

Η ικανότητα ελέγχου των τρεχόντων συστημάτων ανίχνευσης και πρόληψης εισβολών υιοθετήθηκε με την δημιουργία υβριδικής μεθόδου. Η υβριδική μέθοδος έχει την δυνατότητα να ανιχνεύει επιθέσεις οι οποίες προωθούνται από έναν επίμονο επιτιθέμενο οποίος προσπαθεί να αλλάξει την συμπεριφορά των σχεδίων-προτύπων.

Επίσης, η υβριδική μέθοδος είναι ικανή να σταματήσει μια επίθεση εισβολέα από την επιτυχία, δηλαδή να μπορέσει ο εισβολέας να αλλοιώσει ή καταστρέψει πληροφορίες.

Τέλος, γίνεται μια αναφορά στην σύγκριση και υλοποίηση ανίχνευσης και πρόληψης εισβολών. Δηλαδή πως μπορούμε να προστατέψουμε με κρυπτογράφηση μια πληροφορία από ένα εισβολέα. Με την συνεχόμενη κρυπτογράφηση η πληροφορία θα έχει διαφορετικό κλειδί και με αυτόν τον τρόπο ο εισβολέας δεν θα μπορεί να αλλοιώσει ή να καταστρέψει την πληροφορία η οποία μεταφέρεται.

Κεφάλαιο 1: Σύστημα ανίχνευσης και πρόληψης εισβολών

1.1 Εισαγωγή

Η σημερινή εποχή χαρακτηρίζεται περισσότερο από κάθε άλλη ως η εποχή της τεχνολογίας και της πληροφορίας. Παντού γύρω μας βλέπουμε πλέον τη χρήση των υπολογιστών να γίνεται ανάγκη στην καθημερινότητά μας: εργαζόμαστε, επικοινωνούμε, συναλλασσόμαστε και διασκεδάζουμε έχοντας ως μέσο τον υπολογιστή και κατ' επέκταση την ανταλλαγή πληροφοριών. Είναι απαραίτητο γι αυτό το σκοπό τα σύγχρονα Πληροφοριακά Συστήματα (ΠΣ, όπως βάσεις δεδομένων, δίκτυα υπολογιστών, κλπ) να είναι όσο το δυνατόν ασφαλέστερα για τη σωστή τους λειτουργία και αξιοποίηση.

Ένα σημαντικό πρόβλημα στα σύγχρονα δίκτυα υπολογιστών είναι η ασφάλεια των πληροφοριών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, δυστυχώς όμως αυξάνει σημαντικά τα προβλήματα σχετικά με τη διαθεσιμότητα των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μιας επιχείρησης ή ενός οργανισμού. Είναι ιδιαίτερα σημαντικό στις μέρες μας γιατί πολύ συχνά το σύνολο των παρεχόμενων υπηρεσιών μιας επιχείρησης στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας).

Η ασφάλεια ενός Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Επίσης σχετίζεται με την ικανότητα του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Αυτή η ικανότητα στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων, καθώς και στην αδιάλειπτη λειτουργία του δικτύου.

Η ασφάλεια στα δίκτυα υπολογιστών διαπραγματεύεται την ανίχνευση και πρόληψη μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου. Συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με την :

- Πρόληψη (prevention): Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- Ανίχνευση (detection): Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιόν προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- Αντίδραση (reaction): Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απόρρητου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί.[24]

1.2. Σύστημα ανίχνευσης εισβολών

Το Σύστημα ανίχνευσης εισβολών (Intrusiondetectionsystem,IDS) είναι ένα σύστημα παρακολούθησης και ανάλυσης συμβάντων, τα οποία λαμβάνουν χώρα τόσο στους ίδιους τους ηλεκτρονικούς υπολογιστές όσο και στα δίκτυα υπολογιστών. Το σύστημα ανίχνευσης εισβολών είναι ευρύτερα γνωστό με την αγγλική του ορολογία ως Intrusiondetectionsystem.

Τα συστήματα ανίχνευσης εισβολών (IDS) αρχικά χρησιμοποιήθηκαν για την ανάλυση της κυκλοφορίας ενός δικτύου αναζητώντας ενδείξεις επιθέσεων. Ωστόσο, με διαρκώς αυξανόμενο ρυθμό, τα συστήματα αυτά άρχισαν να χρησιμοποιούνται για την εξέταση των αρχείων καταγραφής και την ανάλυση των χαρακτηριστικών των αρχείων, στην προσπάθεια τους να εξακριβώσουν εάν τα αρχεία έχουν παραβιαστεί.[48]

Τα συστήματα IDS χρησιμοποιούντα σαν δολώματα (honeypot), δηλαδή σαν ένα ψεύτικο δίκτυο που χρησιμοποιείται για να προσελκύσει τους επιδόξους εισβολείς και να αποσπάσει την προσοχή τους από το πραγματικό δίκτυο, ενώ οι ενέργειες τους παρακολουθούνται. Στόχος του συστήματος είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες επίθεσης, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Εάν το IDS ανίχνευση μια πιθανή προσπάθεια επίθεσης, τότε προσπαθεί να κάνει ταυτοποιήσεις (αν είναι δυνατόν) και, τέλος προσπαθεί να αντιδράσει ανάλογα.

Οι προσπάθειες παράκαμψης των μηχανισμών ασφάλειας μπορεί να προέρχονται από εξωτερικούς χρήστες, προς το εσωτερικό εταιρικό δίκτυο, στους οποίους δεν επιτρέπεται η πρόσβαση στο υπάρχον πληροφοριακό σύστημα. Επίσης, οι προσπάθειες παράκαμψης πιθανόν να προέρχονται από εσωτερικούς χρήστες, με περιορισμένα δικαιώματα. Τα IDS διαχωρίζονται σε ενεργά και παθητικά.

Τα ενεργά IDS προσπαθούν να μπλοκάρουν τις επιθέσεις, αποκρίνονται με αντίμετρα ή τουλάχιστον προειδοποιούν τους διαχειριστές, κατά την εξέλιξη της επίθεσης. Τα παθητικά IDS απλώς καταγράφουν την εισβολή ή δημιουργούν ίχνη παρακολούθησης, τα οποία γίνονται εμφανή αφού επιτύχει η επίθεση. Ενώ τα παθητικά συστήματα μπορούν να θεωρηθούν άχρηστα στο να αποτρέπουν επιθέσεις, υπάρχουν αρκετές ενδείξεις επιθέσεων, οι οποίες γίνονται εμφανείς μόνο μετά την ολοκλήρωση μιας εισβολής. Για παράδειγμα, αν ένας δυσαρεστημένος διαχειριστής δικτύου του δικτύου υπολογιστών μιας επιχείρησης αποφασίσει να επιτεθεί στην επιχείρηση, θα έχει όλα τα κλειδιά και τους κωδικούς πρόσβασης που είναι αναγκαίοι για να συνδεθεί. Κανένα ενεργό σύστημα δεν θα προειδοποιήσει για αυτήν του την ενέργεια. Τα παθητικά IDS μπορούν όμως να ανιχνεύσουν τις αλλαγές που κάνει ένας διαχειριστής σε συστήματα αρχείων, τις διαγραφές ή όποια άλλη καταστροφή προκαλέσει.[49]

1.2.1. Τι προσφέρουν τα IDS

Τα συστήματα IDS ανιχνεύουν επιθέσεις και άλλες παραβιάσεις ασφάλειας που δεν ανιχνεύονται από άλλα μέτρα προστασίας. Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ένα ή περισσότερα συστήματα, όταν διάφορες, γνωστές αδυναμίες

ασφάλειας των συστημάτων αυτών δεν έχουν διορθωθεί. Παρόλο που κάθε διαχειριστής (administrator) πρέπει και μπορεί σχετικά εύκολα να διορθώνει τις αδυναμίες αυτές, για πολλούς λόγους αυτό δεν συμβαίνει.

Τα IDS ανιχνεύουν αναγνωριστικές ενέργειες που προηγούνται μίας επίθεσης. Για την πραγματοποίηση μίας επίθεσης συνήθως υπάρχουν κάποια στάδια που προηγούνται αυτής. Ο επιτιθέμενος πρώτα εξετάζει τον υποψήφιο στόχο του, ώστε να συγκεντρώσει πληροφορίες για αυτόν και να εντοπίσει ένα σημείο εισόδου, το οποίο θα του επιτρέψει να πραγματοποιήσει την επίθεση με επιτυχία. Αυτό επιτυγχάνεται μέσω του <<Scanning>>. Δίχως την ύπαρξη ενός IDS, ο επιτιθέμενος είναι πολύ πιθανόν να πραγματοποιήσει τις αναγνωριστικές του κινήσεις ανενόχλητος και χωρίς να γίνει αντιληπτός. Ένα IDS θα είχε την δυνατότητα να εντοπίσει τις κινήσεις αυτές του επιτιθέμενου και να πάρει κάποια μέτρα, όπως να καταγράψει το γεγονός, να ειδοποιήσει τους υπεύθυνους ασφάλειας και να εμποδίσει τους επιτιθέμενους να τις ολοκληρώσει.

Ακόμα, συγκεντρώνουν πληροφορίες που αφορούν επιθέσεις που έχουν πραγματοποιηθεί, οι οποίες θα βοηθήσουν στην αποκατάσταση των συστημάτων που παραβιάστηκαν και στην διόρθωση αδυναμιών και παραλήψεων στα ήδη υπάρχοντα μέτρα ασφάλειας. Ακόμα και στην περίπτωση που ένα IDS δεν μπορεί να εμποδίσει την επίθεση, μπορεί να συλλέξει πληροφορίες και στοιχεία για αυτήν που θα χρησιμοποιήσουν τόσο για την αποκατάσταση του συστήματος και την διόρθωση των αδυναμιών ασφάλειας του, όσο και για τον εντοπισμό του επιτιθέμενου και την ποινική δίωξη του.

Επίσης, όταν ένα σύστημα προστατεύεται από ένα IDS τότε ο υποψήφιος επιτιθέμενος διστάζει να πραγματοποιήσει επίθεση. Τέλος, με την χρήση των IDS συλλέγονται πληροφορίες και παρατηρούνται <<patterns>> από ενέργειες που πραγματοποιούνται καθημερινά εναντίον ενός δικτύου και των συστημάτων του, τα οποία μπορούν να βοηθήσουν στην σχεδίαση πιο αξιόπιστων μέτρων ασφαλείας, προσαρμοσμένων ώστε να αντιμετωπίζουν τα γεγονότα και τους κινδύνους που απειλούν το συγκεκριμένο δίκτυο, και να οδηγήσουν στην αποτελεσματικότερη προστασία του.

1.2.2. Πλεονεκτήματα των IDS

Το συστήματα IDS είναι σημαντικό για ένα δίκτυο γιατί μπορεί να ανιχνεύσει εύκολα μια επίθεση εισβολέων. Ένα τέτοιο σύστημα ανιχνεύει απειλές και επιθέσεις. Δεν απαιτείται να προστεθεί κάποιο πρόσθετο υλικό. Το σύστημα IDS μπορεί να ανιχνεύει επιθέσεις που δεν αφορούν το δίκτυο και επιθέσεις δικτύου που δεν είναι ορατές.

Εάν το σύστημα IDS ανιχνεύσει μια επίθεση, τότε υποβάλει πληροφορίες σχετικά για την επίθεση. Μόλις ανιχνευτεί η επίθεση από το σύστημα, λαμβάνονται τα σωστά μέτρα για την αντιμετώπιση της επίθεσης. Ακόμα, το σύστημα IDS αποθηκεύει τις επιθέσεις τις οποίες έχει δεχτεί το σύστημα.

Τα συστήματα αυτά μπορούν να εντοπίσουν εύκολα τις επιθέσεις, οι οποίες έχουν ξεφύγει από τα scanners του host-based αισθητήρες. Ανιχνεύει σε πραγματικό χρόνο την εισβολή, έτσι ώστε να δίνει στον εισβολέα μια ευκαιρία για την αφαίρεση των στοιχείων της επίθεση. Τέλος, το σύστημα IDS επιβεβαιώνει την επιτυχία μιας επίθεσης στο σύστημα.

1.2.3. Μειονεκτήματα των IDS

Όμως το σύστημα IDS έχει και κάποια μειονεκτήματα στη λειτουργία του. Σε περίπτωση που δεχθεί μια επίθεση την οποία δεν κατάφερε να αντιμετωπίσει δεν μπορεί να δώσει μια αυτοματοποιημένη λύση. Ακόμα, το σύστημα IDS δεν μπορεί να διερευνήσει ή να αποτρέψει την επίθεση που έχει δεχθεί.

Το σύστημα IDS εξετάζει τη δικτυακή σύνδεση στον τομέα που είναι συνδεδεμένο και μόνο. Δεν μπορεί να ανιχνεύσει μια επίθεση που γίνεται σε διαφορετικό τμήμα του δικτύου. Συνήθως, χρησιμοποιούν ανάλυση signatures για να καλύψουν τις προδιαγραφές απόδοσης. Έτσι ανιχνεύονται κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αυτή η μέθοδος δεν είναι επαρκής για πιο πολύπλοκα είδη επιθέσεων.

Ένα IDS δεν μπορεί να είναι μια σωστή αντικατάσταση για ένα firewall ή ένα καλό πρόγραμμα προστασίας από ιούς. Ένα IDS θα πρέπει να θεωρηθεί ως εργαλείο για

χρήση σε συνδυασμό με τα τυποποιημένα προϊόντα ασφαλείας (όπως anti-virus και firewall) για να αυξήσει το σύστημά σας ειδικές ή ολόκληρο το δίκτυο ασφαλείας.

Το σύστημα IDS δεν μπορεί να διαχειριστεί αστοχίες υλικού για παράδειγμα εκεί όπου έχει εγκατασταθεί το σύστημα έχει σφάλμα υλικού. Τέλος, θα πρέπει να γίνονται περιοδικοί έλεγχοι στο σύστημα IDS.

1.3. Σύστημα πρόληψης εισβολής

Το σύστημα πρόληψης εισβολών (Intrusionspreventionsystem,IPS) είναι ένα σύστημα ασφάλειας δικτύου όπου παρακολουθεί το δίκτυο ή τη δραστηριότητα του συστήματος για κάποια κακόβουλη δραστηριότητα. Το σύστημα πρόληψης εισβολών είναι ευρύτερα γνωστό με την αγγλική του ορολογία ως Intrusionpreventionsystem.

Τα συστήματα Intrusionspreventionsystems (IPS) εφευρέθηκαν για να επιλύσουν τις ασάφειες στον παθητικό έλεγχο δικτύων με την τοποθέτηση των συστημάτων ανίχνευσης στη σειρά. Μια διαφορά από τις τεχνολογίες των firewall είναι ότι τα IPS ελέγχουν την πρόσβαση ανάλογα την εφαρμογή, παρά τη διεύθυνση IP ή τις πόρτες. Μερικά IPS συστήματα μπορούν επίσης να αποτρέψουν την χρήση επιθέσεων που δεν έχουν ακόμα ανακαλυφτεί (zerodayexploit) που προκαλούνται από Bufferoverflow.[26]

Οι κύριες λειτουργίες του συστήματος πρόληψης είναι να προσδιορίσουν την κακόβουλη δραστηριότητα, να καταγραφούν οι πληροφορίες σχετικά με την δραστηριότητα αυτή, και να προσπαθήσουν να την εμποδίσουν ή να την σταματήσουν. Τα συστήματα πρόληψης εισβολών τοποθετούνται σε σειρά και είναι σε θέση να συμμετάσχουν ενεργά στην πρόληψη εισβολών που εντοπίζονται.

Ένα σύστημα πρόληψης είναι οποιαδήποτε συσκευή που ελέγχει την κάθε πρόσβαση για να προστατεύσει τους υπολογιστές από τους hackers. Η τεχνολογία "Intrusionprevention" θεωρείται από μερικούς μια επέκταση της τεχνολογίας Intrusiondetection (IDS) επειδή και τα δυο συστήματα δραστηριοποιούνται στο δίκτυο και στο σύστημα., αλλά είναι πραγματικά μια άλλη μορφή ελέγχου πρόσβασης, όπως ένα firewall για κάθε εφαρμογή.

Πιο συγκεκριμένα, το σύστημα πρόληψης εισβολών μπορεί να κάνει τέτοιες ενέργειες, όπως να στείλει μια ειδοποίηση, να κάνει επαναφορά της σύνδεσης και να παρεμποδίσει την παραβίαση μιας εφαρμογής. Το σύστημα πρόληψης εισβολών είναι σίγουρα το επόμενο επίπεδο της τεχνολογίας για ασφάλεια με την ικανότητα του να παρέχει ασφάλεια σε όλα τα επίπεδα του συστήματος από τον πυρήνα του λειτουργικού συστήματος στο δίκτυο πακέτων δεδομένων.

Παρέχει τις πολιτικές και τους κανόνες για την κυκλοφορία του δικτύου ,μαζί με το IDS, για το σύστημα ειδοποίησης ή διαχείρισης του δικτύου για ύποπτη κίνηση, αλλά επιτρέπει στο διαχειριστή να παρέχει την ενέργεια από την οποία ειδοποιείται.

Όταν το σύστημα πρόληψης εισβολών καταλάβει ότι δέχεται επίθεση τότε κάνει προσπάθειες για να την σταματήσει. Το σύστημα πρόληψης εισβολών έχει την ικανότητα να αποτρέψει γνωστές υπογραφές εισβολής, αλλά και κάποιες άγνωστες επιθέσεις λόγω δεδομένων της γενικής συμπεριφοράς της επίθεσης. Το σύστημα πρόληψης εισβολών θεωρείται η <<επόμενη γενιά>> του IDS.[25]

1.3.1. Τι προσφέρουν τα IPS

Τα συστήματα IPSπαρέχουν μια ποικιλία δυνατοτήτων ασφαλείας. Το σύστημα IPS είναι ένας προηγμένος ευφυής τρόπος ελέγχου των ευπαθειών. Αποτελείται από πολλές τεχνικές για να εξασφαλιστεί το βέλτιστο και το πιο προηγμένο επίπεδο ασφάλειας.

Τα συστήματα IPS ελαχιστοποιούν τις ψευδώς θετικά υπογραφές εισβολής και αυξάνουν την ακρίβεια αναγνώρισης απειλής εφαρμόζοντας υπογραφές μόνο σε σχετικά τμήματα κίνησης του δικτύου που καθορίζεται από το αρμόδιο πρωτόκολλο. ΤοIPS προστατεύει ενεργά το δίκτυο από εισβολείς.

Επίσης, χρησιμοποιεί προηγμένους κανόνες εύρεσης που μπορεί να αποτρέψει ακόμα και zero-day επιθέσεις. Η βάση δεδομένων ενημερώνετε πολλές φορές κάθε μέρα με τους πιο πρόσφατους ορισμούς υπογραφών. Το σύστημα IPS βελτιώνει την ασφάλεια του λειτουργικού συστήματος και στηρίζει τις επιχειρηματικές διαδικασίες με το ρόλο του διαχειριστή που επιτρέπει την εκχώρηση περισσότερων από 100

διαφορετικών δραστηριοτήτων με μοναδικά δικαιώματα για διαφορετικούς διαχειριστές.

Επίσης, το IPS εκτελεί εκτενή καταγραφή των δεδομένων που σχετίζονται με συμβάντα που εντοπίστηκαν και μπορεί να ανιχνεύσει διάφορα είδη των ύποπτων δραστηριοτήτων. Περιλαμβάνει ανάλυση κώδικα, ανάλυση της κυκλοφορίας του δικτύου, το φιλτράρισμα της κυκλοφορίας του δικτύου, το αρχείο σύστημα παρακολούθησης, καταγραφής και ανάλυσης του δικτύου παρακολούθησης της διαμόρφωσης.

Το σύστημα IPS έχει ευρεία προστασία για τον Web, Mail, Ftp, Windows, Linux, BSD, UNIX, Routers, Firewalls, βάσεις δεδομένων όπως DB2, Oracle, MySQL, MSsql, Postgresql.Τέλος, το IPS προστατεύει το σύστημα προληπτικά από απειλές και προσπαθεί να βελτιώσει τη στάση ασφάλειας μέσα από αποδεκτή χρήση εφαρμογής.

1.3.2. Πλεονεκτήματα των IPS

Το συστήματα IPS είναι σημαντικό για ένα δίκτυο γιατί μπορεί να εντοπίσει εύκολα μια επίθεση εισβολέων. Τα συστήματα IPS παρέχουν σε πραγματικό χρόνο ειδοποιήσεις για τυχόν παραβίαση του δικτύου δίνοντας τη δυνατότητα στο προσωπικό να ανταποκριθεί και να μετριάσει αυτόν τον κίνδυνο.

Παρέχει τακτικές ενημερώσεις ανίχνευσης απειλών για να εξασφαλιστεί ότι τα συστήματα προστατεύονται από τις πιο πρόσφατες απειλές. Είναι σε θέση να εισπράξει τα αρχεία καταγραφής του συστήματος από όλες τις συσκευές του δικτύου και να συσχετιστούν και να επιθεωρούν χρησιμοποιώντας μία κονσόλα διαχείρισης. Μπορεί να εντοπίσει τις επιθέσεις που δεν μπορεί να ανιχνευθεί από το δίκτυο με βάση το IDS, επειδή είναι συνήθως κωδικοποιημένο.

1.3.3. Μειονεκτήματα των IPS

Όμως το σύστημα IPS έχει και κάποια μειονεκτήματα στη λειτουργία του. Το σύστημα IPS είναι λιγότερο αποδοτικό. Δεν μπορεί να ανιχνεύσει μικρότερες

εκδηλώσεις του δικτύου επιπέδου. Επίσης, δεν μπορεί να εξετάσει καμία κρυπτογραφημένη κίνηση.

Το IPS δεν θα πρέπει να χρησιμοποιείται με πολλαπλά λειτουργικά συστήματα. Θα πρέπει το IPS να έχει αισθητήρες σφαλμάτων διαφορετικά δημιουργεί αρνητικές επιπτώσεις στη κίνηση του δικτύου.

Το λογισμικό μπορεί να δημιουργήσει ένα μεγάλο αριθμό λανθασμένων συναγερμών. Αυτές οι ψευδείς συναγερμοί αυξάνονται σε δίκτυα όπου υπάρχει μεγάλος αριθμός χρηστών. Για την αποφυγή ψευδών συναγερμών, οι επαγγελματίες πρέπει να λαμβάνουν εκτενή κατάρτιση, έτσι ώστε να μπορούν να αναγνωρίζουν ποιος είναι ο ψευδής συναγερμό και ποιος δεν είναι. Η δαπάνη για την ολοκλήρωση αυτής της εκπαίδευσης είναι ένα άλλο μειονέκτημα του λογισμικού πρόληψης εισβολών.

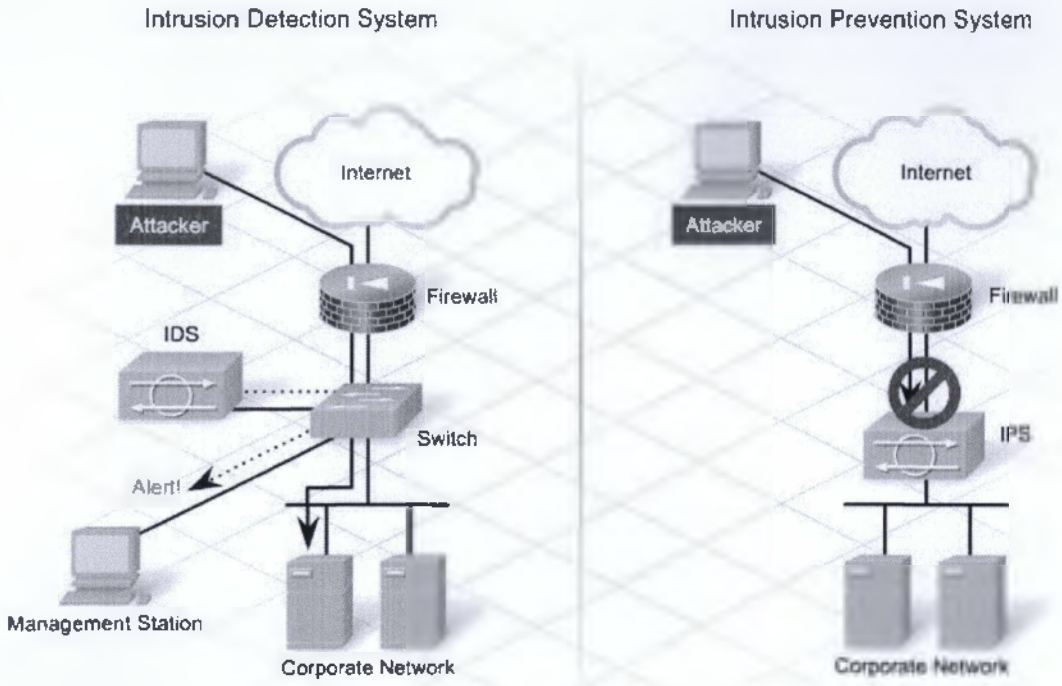
1.4. Διαφορά μεταξύ IDS και IPS συστήματα

Τα IDS και IPS αρχικά αναπτύχθηκαν για την αντιμετώπιση των απαιτήσεων που έλειπαν στα περισσότερα firewalls. Τα IDS βασικά χρησιμοποιήθηκαν για την ανίχνευση των απειλών ή εισβολών σε τμήμα του δικτύου. Αλλά τα IPS εστίαζαν στον εντοπισμό των απειλών αυτών ή εισβολών για τον αποκλεισμό ή την πτώση των δραστηριοτήτων τους. Τα IDS και IPS είναι μια λίστα από παρόμοιες λειτουργίες, όπως έλεγχος των πακέτων, stateful ανάλυση, επανασυναρμολόγηση τμήματος TCP, βαθύς έλεγχος των πακέτων, επιβεβαίωση πρωτοκόλλου και αντιστοίχιση υπογραφής.

Το καλύτερο παράδειγμα για την πύλη της ασφαλείας στην διάρκεια της διαφοράς του IDS και IPS είναι, ένα IDS λειτουργεί σαν ένα περιπολικό εντός των συνόρων, παρακολούθηση τις δραστηριότητες και ψάχνει για ανώμαλες καταστάσεις. Αλλά ένα IPS λειτουργεί σαν ένα φύλακα στην πύλη που επιτρέπει και παρεμποδίζει την πρόσβαση με βάση τις πιστοποιήσεις και κάποιο προκαθορισμένο σύνολο κανόνων, ή την πολιτική. Δεν έχει σημασία πόσο ισχυρή είναι η ασφάλεια στην πύλη, οι περιπολίες συνεχίζουν να λειτουργούν σε ένα σύστημα που παρέχει τους δικούς του ελέγχους.

Τα δύο συστήματα είναι διαφορετικά όπου το ένα είναι ένα παθητικό σύστημα παρακολούθησης ανίχνευσης και το άλλο είναι ένα ενεργό σύστημα πρόληψης. Η

πανάρχαια συζήτηση του γιατί θέλετε να θα είναι παθητική, όταν θα μπορούσε να είναι ενεργή μπαίνει στο παιχνίδι. Μπορείτε να αξιολογήσει επίσης την εφαρμογή μιας πιο ώριμη τεχνολογία IDS, σε σχέση με τους νεότερους, λιγότερες εγκατεστημένες λύσεις IPS.[23]



Εικόνα 1: Διαφορές μεταξύ IDS και IPS

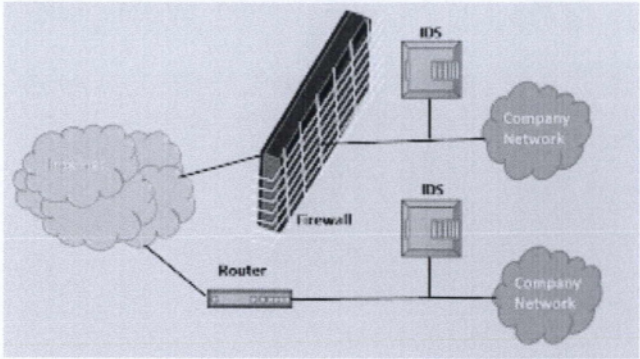
ΚΕΦΑΛΑΙΟ 2:Συστήματα ανίχνευσης εισβολών

2.1 Ορισμός IDS

Τα συστήματα ανίχνευσης εισβολών (IDS) βοηθούν τα συστήματα πληροφοριών για να προετοιμαστούν και να αντιμετωπίσουν τις επιθέσεις. Αυτό θα ολοκληρωθεί με τη συλλογή πληροφοριών από μια ποικιλία συστημάτων και δικτύων, και την ανάλυση πληροφοριών για πιθανά προβλήματα ασφάλειας. Ένα IDS είναι ένα σύστημα υψηλής τεχνολογίας ισοδύναμο με ένα σύστημα συναγερμού, το οποίο έχει ρυθμιστεί να παρακολουθεί τις πύλες εισόδου πληροφόρησης, εχθρικές δραστηριότητες και γνωστούς εισβολείς.

Ένα IDS αποτελείται από αρχεία όπως routers, firewalls και serves, τοπικά αρχεία του συστήματος τα οποία ζητούν πρόσβαση, ροή δεδομένων και πολλά άλλα. Επιπλέον, τα IDS αποθηκεύουν συχνά μια βάση δεδομένων των γνωστών υπογραφών επίθεσης και τα συγκρίνει με μοτίβα δραστηριότητας ή με τη συμπεριφορά που βλέπει στα δεδομένα. Έτσι, τα IDS μπορούν να εκδίδουν ειδοποιήσεις ή προειδοποιήσεις, να λαμβάνει διάφορα είδη αυτοματοποιημένων ενεργειών που κυμαίνονται από το κλείσιμο των συνδέσεων στο Internet και να κάνει άλλες δραστικές προσπάθειες για τον εντοπισμό εισβολέων ώστε να συλλέγουν αποδείξεις των φαύλων δραστηριοτήτων τους.

Κατ' αναλογία, αυτό που κάνει ένα IDS για το δίκτυο είναι αυτό που κάνει ένα πακέτο λογισμικού antivirus για τα αρχεία που εισάγει ένα σύστημα. Τα IDS ελέγχουν το περιεχόμενο της κίνησης του δικτύου για να αναζητήσουν και να εκτρέψουν πιθανές επιθέσεις, όπως ακριβώς και ένα πακέτο προστασίας από ιούς το οποίο ελέγχει το περιεχόμενο των εισερχομένων αρχείων, τα συνημμένα emails, το ενεργό περιεχόμενο στο παγκόσμιο ιστό, για να ψάξουν για υπογραφές ιών ή για πιθανές κακόβουλες ενέργειες (πρότυπα συμπεριφοράς που είναι τουλάχιστον ύποπτο).



Εικόνα 2: Λειτουργία IDS

Ένα IDS έχει σχεδιαστεί και χρησιμοποιείται για την ανίχνευση επιθέσεων ή μη εξουσιοδοτημένων χρήση συστημάτων, δικτύων και σχετικών πόρων, ακόμα και για να εκτρέψουν αυτές τις επιθέσεις. Ένα σύστημα IDS μπορεί να τρέχει στις ίδιες συσκευές ή serves όπου λειτουργούν firewalls.[50]

2.1.1. Το IDS προβλέπει τα εξής:

- Παρακολούθηση και ανάλυση των χρηστών και τη δραστηριότητα του συστήματος.
- Έλεγχος των διαμορφώσεων του συστήματος και τα τρωτά σημεία.
- Η αξιολόγηση της ακεραιότητας των κρίσιμων σημείων του συστήματος και τα αρχεία δεδομένων.
- Στατιστική ανάλυση των μοντέλων δραστηριότητας.

2.1.2. Χαρακτηριστικά των συστημάτων ανίχνευσης εισβολών

Τα IDS θα πρέπει να έχουν τα εξής χαρακτηριστικά:

- Θα πρέπει να τρέχουν συνεχώς, χωρίς ανθρώπινη επίβλεψη. Το σύστημα πρέπει να είναι αξιόπιστο για να μπορέσει να τρέξει στο παρασκήνιο.
- Πρέπει να είναι ανεκτικό σε σφάλματα, υπό την έννοια ότι πρέπει να επιβιώσει μια κατάρρευση του συστήματος και να μην έχουν βάση γνώσης ότι ανοικοδομήθηκε κατά την επανεκκίνηση.
- Το σύστημα θα πρέπει να είναι σε θέση να παρακολουθεί τον εαυτό του για να εξασφαλίσει ότι δεν έχει παρεκτραπεί.

- Θ πρέπει να επιβάλει ελάχιστη επιβάρυνση για το σύστημα, που σημαίνει ότι δεν θα πρέπει να επιβραδυνθεί ο υπολογιστής.
- Κάθε σύστημα έχει ένα διαφορετικό πρότυπο χρήστη, και ο αμυντικός μηχανισμός θα πρέπει να προσαρμοστεί εύκολα σε αυτά τα πρότυπα.
- Θα πρέπει να αντιμετωπίσουν την αλλαγή της συμπεριφοράς του συστήματος με την πάροδο του χρόνου, όπως νέες εφαρμογές που μπορεί να προστεθεί. Το προφίλ του συστήματος θα αλλάξει με την πάροδο του χρόνου, και τα IDS θα πρέπει να είναι σε θέση να προσαρμοστούν.

2.1.3. Πλεονεκτήματα και μειονεκτήματα IDS

Δεν υπάρχει αμφιβολία ότι ένα σύστημα ταυτότητας είναι εξαιρετικά σημαντικό για τη διατήρηση της ασφάλειας του δικτύου από κακόβουλες δραστηριότητες, το οποίο είναι απαραίτητο για τα μεγάλα δίκτυα επιχειρήσεων. Ένα από τα μεγάλα πλεονεκτήματα των συστημάτων αυτών είναι ότι δραστηριοποιούνται όλο το εικοσιτετράωρο , πράγμα που σημαίνει ότι ακόμα όταν και ο χρήστης βρίσκεται μακριά από το πληκτρολόγιο ή κοιμάται τα συστήματα γνωρίζουν κακόβουλες δραστηριότητες.

Άλλο μεγάλο πλεονέκτημα είναι το ευέλικτο των συστημάτων. Μπορούν να προσαρμοστούν σε χρήστες που το χρειάζονται και να τους επιτρέψει προσαρμοσμένη ασφάλεια του δικτύου. Το μεγάλο μειονέκτημα του συστήματος ανίχνευσης εισβολών είναι η αδυναμία τους να διακρίνουν μια κακόβουλη δραστηριότητα από μια φιλική δραστηριότητα που σημαίνει ότι όταν, για παράδειγμα, ένας φίλος αποκτήσει πρόσβαση στο δίκτυο μας, δεν μπορεί να διακρίνει εάν είναι κακόβουλο ή όχι και κλειδώσει το δίκτυο

2.1.4. Βασικοί τύποι του συστήματος IDS

Υπάρχουν δυο βασικοί τύποι του συστήματος IDS. Το Host-Based Intrusion Detection Systems (HIDS) καιτο Network Intrusion Detection Systems (NIDS).

Host-Based Intrusion Detection Systems (HIDS)

Τα Host-based συστήματα ανίχνευσης εισβολών αποτελείται από αισθητήρες που βρίσκονται σε serves ή θέσεις εργασίας για την ανίχνευση επιθέσεων στο συγκεκριμένο σταθμό εργασίας ή διακομιστή. Ο παράγοντας HIDS ή ο αισθητήρας τοποθετείται πάνω ή κοντά σε μια υπηρεσία διακομιστή. Όπως HIDSs παρακολουθούν ένα συγκεκριμένο σταθμό εργασίας ή διακομιστή, τοποθετούνται ως λογισμικό στο λειτουργικό σύστημα του ξενιστή.

Τα είδη των δραστηριοτήτων παρακολούθησης που εκτελούνται από HIDSs είναι host-centric εκδηλώσεις, όπως κακόβουλο κώδικα εκτελέσεις, πλήθος ανάλυση καταγραφής, το αρχείο παρακολούθησης του συστήματος και του δικτύου παρακολούθηση της διαμόρφωσης. Καθώς επιθέσεις που περιλαμβάνουν τα προαναφερθέντα γεγονότα μπορεί να είναι είτε εσωτερικές ή εξωτερικές, HIDSs είναι ιδιαίτερα ευέλικτο, όταν πρόκειται για την καταπολέμηση των απειλών και από τις δύο εντός και εκτός του δικτύου.

Πλεονεκτήματα HIDS:

- Τα HIDSs εντοπίζουν τις επιθέσεις με μεγαλύτερη ακρίβεια και δημιουργούν λιγότερους ψευδείς συναγερμούς, καθώς απασχολούν συστήματα καταγραφής που περιέχουν γεγονότα που έχουν ήδη συμβεί. Ενώ τα NIDSs είναι πιο γρήγορα για την αντιμετώπιση απειλών όπως αναλύουν την κίνηση του δικτύου σε πραγματικό χρόνο, όμως παράγουν περισσότερα ψευδώς θετικά αποτελέσματα.
- Τα HIDSs περιέχουν αρχεία δραστηριότητας πρόσβασης, σύνδεσης/αποσύνδεσης δραστηριότητας, άπειρες εγκαταστάσεις εκτελέσιμων αρχείων, δραστηριότητας υποδοχής στο δίκτυο όπου επιτρέπει στο HIDS να παράγουν πληροφορίες που δεν παρέχονται από το NIDS.
- Μπορούν να καθορίσουν εάν ή όχι ένας συναγερμός μπορεί να επηρεάσει το συγκεκριμένο σύστημα.
- Λειτουργεί σε κρυπτογραφημένο περιβάλλον.
- Τα HIDSs εντοπίζουν επιθέσεις τις οποίες δεν μπορούν να εντοπίσουν τα NIDS, και κάνει αλλαγές στα αρχεία του συστήματος από την κονσόλα του συστήματος. Αυτό το καθιστά πιο αποτελεσματικό όταν πρόκειται για την προστασία των οικοδεσποτών από εσωτερικούς χρήστες σε σύγκριση με το NIDS

- Τέλος, όπως αναφέρθηκε το HIDSs είναι το λογισμικό που διατίθεται στους οικοδεσπότες και εκ τούτου δεν απαιτούν κάποιο συγκεκριμένο υλικό.

Μειονεκτήματα HIDS:

- Τα IDS πρέπει να έχουν μια διεργασία σε κάθε σύστημα που θέλετε να παρακολουθήσετε.
- Τα IDS μπορεί να έχουν υψηλό κόστος ιδιοκτησίας και συντήρησης.
- Η IDS χρησιμοποιεί τοπικούς πόρους του συστήματος.
- Τα ID, εάν είστε συνδεδεμένοι σε κάποιο τοπικό επίπεδο, θα μπορούσε να τεθεί σε κίνδυνο ή να απενεργοποιηθεί.
- Δεν προστατεύει το σύνολο της υποδομής.

Network Intrusion Detection Systems (NIDS)

Τα συστήματα ανίχνευσης NetworkIntrusion τοποθετείται σε ένα δίκτυο για την ανάλυση της κίνησης για τα ανεπιθύμητα ή κακόβουλα γεγονότα. Σε αντίθεση με το HIDS, ένα NIDS μπορεί ή δεν μπορεί να έχει το υλικό που συνδέονται με αυτό. Εάν δεν έχει το υλικό, τότε το υλικό θα είναι ένα ειδικό IDS. Σε αντίθετη περίπτωση, το NIDS μπορεί να είναι το λογισμικό-μόνο και ο χρήστης να είναι υπεύθυνος για τη διάθεση του υλικού.

Το υλικό αποτελείται ουσιαστικά από αισθητήρες που λαμβάνουν τις αποφάσεις ως προς το εάν η κίνηση είναι κακόβουλη. Αισθητήρες μπορούν να τοποθετηθούν μεταξύ των δύο στοιχείων του δικτύου, όπως τα firewall και τα router που σημαίνει ότι ο αισθητήρας θα είναι πίσω από το τείχος προστασίας για το εσωτερικό τμήμα του δικτύου και για την ανάλυση της κίνησης που δεν έχει αποκλειστεί από το τείχος προστασίας. Οι αισθητήρες αυτοί μπορούν να βοηθήσουν στον εντοπισμό επιθέσεις άρνησης υπηρεσίας, επιθέσεις για την κλοπή των πληροφοριών και ανεπιθύμητη κίνηση, όπως απροσδόκητες υπηρεσίες και εκείνων που παραβιάζουν τις πολιτικές.

Πλεονεκτήματα NIDSs:

- Μπορεί να πάρει τις πληροφορίες γρήγορα, χωρίς καμία ρύθμιση των υπολογιστών ή να πρέπει να ανακατευθύνει την καταγραφή των μηχανισμών.

- Τα HIDSs βασίζονται σε αρχεία καταγραφής του συστήματος το οποίο μπορεί να αλλοιωθεί ή να τροποποιηθεί για να αφαιρεθούν τα στοιχεία μιας επίθεσης. Ωστόσο, το NIDSs παρακολουθούν τις κινήσεις που καθιστά σχεδόν αδύνατο στον εισβολέα να αφαιρέσει οποιοδήποτε στοιχείο.
- Τα NIDSs ανιχνεύουν τους εισβολείς σε πραγματικό χρόνο, καθώς παρακολουθούν τις κινήσεις τους το οποίο καθιστά δυνατό για την κατάσταση που πρέπει να διορθωθεί με την ταχύτερη απόκριση, αλλά και μειώνοντας την πιθανότητα το σύστημα να τεθεί σε κίνδυνο.
- Αν εγκατασταθεί πίσω από το τείχος προστασίας, τότε οι ανάγκες μπορούν να χρησιμοποιηθούν ως εργαλείο για την ανίχνευση κινήσεων όπου το τείχος προστασίας απέτυχε να εμποδίσει.
- Δεν επηρεάζει το δίκτυο ή τις πηγές δεδομένων.
- Δεν δημιουργεί επιβάρυνση του συστήματος.

Μειονεκτήματα NIDS:

- Δεν μπορεί να σαρώσει τα πρωτόκολλα, εάν τα δεδομένα είναι κρυπτογραφημένα.
- Μπορεί να συμπεράνει από την κυκλοφορία του δικτύου τι συμβαίνει στο κεντρικό υπολογιστή, αλλά δεν μπορεί να πει το αποτέλεσμα.
- Δύσκολο να εφαρμόσει την πλήρη μεταγωγή των δικτύων.
- Έχει δυσκολία στη διατήρηση του δικτύου με πολύ μεγάλο εύρος ζώνης.

Κάθε ένας από τους τύπους του IDS έχει τα δικά του πλεονεκτήματα και μειονεκτήματα. Για την καλύτερη χρήση ενός συστήματος είναι να συνδυαστούν και οι δυο τύποι IDS μαζί. Γιατί το HIDSs κάνει καλύτερη δουλεία για την προστασία από εσωτερικές επιθέσεις και το NIDSs κάνει καλύτερη δουλειά στην ανίχνευση επιθέσεων που απαιτούν πακέτο ανάλυσης. Συνεπώς, κάθε ένας τύπος βοηθάει τον άλλο.

Δίκτυο συστήματος ανίχνευσης εισβολής και βάση υποδοχής σύστημα ανίχνευσηςεισβολής

2.1.5. Ψευδώς θετικά και αρνητικά των IDS

Είναι αδύνατο για ένα IDS να είναι τέλειο, κυρίως λόγω της κίνησης του δικτύου που είναι τόσο περίπλοκη. Τα λανθασμένα αποτελέσματα σε ένα IDS χωρίζονται σε δύο τύπους: ψευδώς θετικά και ψευδώς αρνητικά. Ψευδώς θετικά συμβαίνουν όταν το IDS εσφαλμένα εντοπίσει κάποιο πρόβλημα με καλοήθη κυκλοφορία. Λάθος αρνητικά αποτελέσματα εμφανίζονται όταν ανεπιθύμητη κίνηση περνάει απαρατήρητα από το IDS. Και οι δύο δημιουργούν προβλήματα για τους διαχειριστές της ασφάλειας και μπορούν να απαιτούν από το σύστημα να βαθμονομηθεί.

Ένας μεγαλύτερος αριθμός των ψευδώς θετικών είναι γενικά πιο αποδεκτή, αλλά μπορεί να επιβαρύνει τον διαχειριστή με επαχθείς ποσότητες δεδομένων. Ωστόσο, απαρατήρητα είναι και τα ψευδώς αρνητικά αποτελέσματα αλλά δεν δίνεται στον διαχειριστή ασφάλειας μια ευκαιρία να επανεξετάσει τα δεδομένα. Όλοι παράγουν ψευδώς θετικά (χαρακτηρίζουν την καλοήθη δραστηριότητα ως κακόβουλο) και ψευδώς αρνητικά αποτελέσματα (παραλείποντας να προσδιορίσει κακόβουλη δραστηριότητα). Πολλές οργανώσεις επιλέγουν να συντονιστείτε IDPSs έτσι ώστε τα ψευδώς αρνητικά να μειωθούν και τα ψευδώς θετικά να αυξηθούν, η οποία απαιτεί πρόσθετους πόρους για την ανάλυση ψευδών θετικών αποτελεσμάτων από τα αληθινά κακόβουλα γεγονότα. Πλέον IDPSs προσφέρουν επίσης χαρακτηριστικά που αντισταθμίζουν για τη χρήση των κοινών τεχνικών φοροδιαφυγής, που τροποποιούν τη μορφή ή το χρονοδιάγραμμα της κακόβουλης δραστηριότητας για να αλλάξει την εμφάνισή του. Πλέον το IDPSs χρησιμοποιείται για πολλαπλές μεθόδους ανίχνευσης, είτε χωριστά είτε ενσωματωμένα, για να παρέχουν πιο ευρεία και ακριβή ανίχνευση.[15]

2.1.6. Περιορισμοί IDS

Ο θόρυβος μπορεί να περιορίσει σημαντικά την αποτελεσματικότητα ενός συστήματος ανίχνευσης εισβολών του. Τα κακός πακέτα που παράγονται από τα σφάλματα λογισμικού, τα διεφθαρμένα στοιχεία DNS, και τα τοπικά πακέτα που διέφυγαν μπορεί να δημιουργήσει ένα σημαντικά μεγάλο ρυθμό εσφαλμένων συναγερμών. Δεν είναι ασυνήθιστο για τον αριθμό των πραγματικών επιθέσεων να είναι πολύ κάτω από το ψευδώς ποσοστό συναγερμού. [50]

Οι πραγματικές επιθέσεις είναι συχνά πολύ κάτω από το ψευδώς ποσοστό συναγερμού που συχνά παραλείπονται και αγνοούνται. Πολλές επιθέσεις είναι προσαρμοσμένες για συγκεκριμένες εκδόσεις λογισμικού που είναι συνήθως απαρχαιωμένη.

2.1.7. Σύστημα ανίχνευσης εισβολών εναντίον Firewalls

Υπάρχει μια λανθασμένη αντίληψη ότι το σύστημα ανίχνευσης εισβολών είναι ένα τείχος προστασίας. Αν και οι δύο ταυτότητες και firewalls είναι συσκευές ασφάλειας του δικτύου, διαφέρουν ως προς τη λειτουργικότητά τους και την προσέγγιση που λαμβάνουν για την παρακολούθηση της κίνησης του δικτύου.

Ένα IDS γενικά ανιχνεύει ανεπιθύμητους χειρισμούς των συστημάτων πληροφορικής. Ένα IDS παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση του δικτύου για πιθανές παραβιάσεις της ασφάλειας, δημιουργεί ένα αρχείο καταγραφής που συνέβη η εκδήλωση, και ενεργοποιεί έναν συναγερμό για διαχειριστές σχετικά με το συμβάν. Οι διαχειριστές μπορούν στη συνέχεια να λάβουν τα κατάλληλα μέτρα για την επίλυση του ζητήματος. Ένα IDS μπορεί μόνο να ανιχνεύει και να προειδοποιεί για παραβίαση προσωπικών στοιχείων.

Ένα τείχος προστασίας είναι μια ειδική εφαρμογή ή λογισμικό που τρέχει σε ένα υπολογιστή, ο οποίος ελέγχει το δίκτυο της διερχόμενης κυκλοφορίας μέσα από αυτό, και αρνείται ή δεν επιτρέπει τη δίοδο που βασίζεται σε ένα σύνολο κανόνων. Ένα τείχος προστασίας, από την άλλη πλευρά, απομονώνει το εσωτερικό δίκτυο από το εξωτερικό, συνήθως το Διαδίκτυο σύμφωνα με την προεπιλεγμένη συμπεριφορά του. Ένα τείχος προστασίας θα μπλοκάρει όλες σχεδόν τις επιθέσεις εκτός εάν ορίζεται διαφορετικά ή έχουν σχεδιαστεί διαφορετικά. Οι διαχειριστές του θα πρέπει να ρυθμίσουν με μη αυτόματο τρόπο τους κανόνες του firewalls για να επιτρέψει ή να αρνηθεί την κίνηση του δικτύου με βάση τον αριθμό των λιμένων, τα πρωτόκολλα, την πηγή ή το εύρος IP διεύθυνση προορισμού, προέλευσης ή προορισμού τομείς, κλπ.

Μια καλή ιδέα είναι να χρησιμοποιηθούν και τα δυο συστήματα τόσο τοπ IDS όσο και το firewalls.Με αυτόν τον τρόπο το IDS θα προειδοποιεί για τις επιθέσεις και το firewalls θα εμποδίζει τις επιθέσεις.

2.1.8. Κορυφαία συστήματα ανίχνευσης εισβολών

Snort	Είναι ένα ελαφρύ δωρεάν σύστημα ανίχνευσης εισβολών, ικανό να εκτελεί σε πραγματικό χρόνο ανάλυση της κυκλοφορίας και καταγραφής πακέτων σε IP δίκτυα.
Bro	Bro είναι μια ανοιχτή πηγή, Unix-based σύστημα ανίχνευσης εισβολών που παρακολουθεί παθητικά την κυκλοφορία του δικτύου και ψάχνει για ύποπτη δραστηριότητα.
Sguil	Sguil είναι μια συλλογή των ελεύθερων συστατικών λογισμικού για παρακολούθηση ασφάλειας δικτύου και την περίπτωση με γνώμονα την ανάλυση των IDS ειδοποιήσεις.

2.2. Εισαγωγή στο Snort

Είναι το πιο δημοφιλές OpenSourceIDS σε χρήση σήμερα. Υποστηρίζει και τα δύο συστήματα Unix και Windows. Λειτουργεί με την εξέταση της κυκλοφορίας που

εισέρχονται στο δίκτυο συνήθως VLANs. Συγκρίνει την κυκλοφορία σε μια βάση δεδομένων των γνωστών υπογραφών επίθεσης και ανώμαλες συμπεριφορές και δημιουργεί μια ειδοποίηση όταν ανιχνεύει μια εισβολή.

Το Snort χρησιμοποιεί κανόνες που είναι αποθηκευμένοι σε αρχεία κειμένων που μπορούν να τροποποιηθούν από ένα συντάκτη κειμένων. Οι κανόνες αυτοί ομαδοποιούνται σε διάφορες κατηγορίες. Οι κανόνες της κάθε κατηγορίας αποθηκεύονται σε ξεχωριστά αρχεία. Αυτά τα αρχεία συμπεριλαμβάνονται σε ένα κύριο αρχείο, το snort.conf. ΤοSnort διαβάζει αυτούς τους κανόνες κατά την εκκίνηση του και διαμορφώνει τις εσωτερικές δομές δεδομένων ή 'τις αλυσίδες' προκειμένου στη συνέχεια να εφαρμόσει αυτούς τους κανόνες στα δεδομένα που θα εξετάσει.

Η εύρεση των υπογραφών και η χρήση τους στους κανόνες είναι μια απαιτητική εργασία, δεδομένου ότι όσο περισσότεροι κανόνες χρησιμοποιούνται, τόσο περισσότερη επεξεργαστική ισχύς απαιτείται για να επεξεργαστούν τα δεδομένα που θα συλλέξει το σύστημα, σε πραγματικό χρόνο. Το Snort έρχεται με ένα πλούσιο σύνολο προκαθορισμένων κανόνων για να ανιχνεύσει την δραστηριότητα παρεισφρήσεων ενώ δίνεται παράλληλα η δυνατότητα να προστεθούν και άλλοι κανόνες. Υπάρχει επίσης η πιθανότητα να διαγραφούν-απενεργοποιηθούν μερικοί από τους ενσωματωμένους κανόνες για αποφευχθούν λανθασμένες ειδοποιήσεις.[22]

2.2.1. Τι είναι το Snort

Το Snort είναι ένα ελαφρύ, ανοιχτού κώδικα σύστημα ανίχνευσης και πρόληψης εισβολών. Έχει την ικανότητα να αναλύει δικτυακή κίνηση σε πραγματικό χρόνο, να ειδοποιεί για πιθανές επιθέσεις, να μπλοκάρει και να καταγράφει πακέτα σε δίκτυα πρωτοκόλλου IP (InternetProtocol). Χρησιμοποιεί ένα συνδυασμό μηχανισμών ανάλυσης των διαφόρων πρωτοκόλλων επικοινωνίας και αναγνώρισης προτύπων με σκοπό να ανιχνεύσει ανωμαλίες, επιθέσεις και άλλες περιπτώσεις κατά τις οποίες γίνεται κακή χρήση του δικτύου. [8]

Snort είναι ένα δίκτυο με βάση το IDS που μπορεί να παρακολουθεί όλη την κυκλοφορία σε μια σύνδεση δικτύου για να ψάξει για ύποπτη κίνηση. Τυπικά, ένα δίκτυο που βασίζεται σε ένα IDS έχει συσταθεί για την παρακολούθηση ενός DMZ ή

το εσωτερικό δίκτυο ακριβώς πίσω από το τείχος προστασίας, ώστε να προειδοποιεί για ενδεχόμενες απειλές ότι το τείχος προστασίας δεν είχε πιάσει.

Το Snort είναι διαθέσιμο υπό GPL, ένα δωρεάν πρόγραμμα που τρέχει σε περιβάλλον Windows και GNU/Linux. Επιπλέον, χρησιμοποιεί μια ευέλικτη γλώσσα κανόνων για να περιγράψει τις δραστηριότητες που μπορούν να θεωρηθούν κακόβουλες. Η μηχανή ανάλυσης και ανίχνευσης του Snort αποτελείται από ένα σύνολο διαφορετικών υποσυστημάτων (plugins) που ενσωματώνονται σε μια ενιαία αρχιτεκτονική. Υπάρχει μια διεπαφή Ιστού που λειτουργεί με Snort που ονομάζεται BASE (BasicAnalysisandSecurityEngine), η οποία βασίζεται στην ACID (AnalysisConsoleforIntrusionDatabases), η οποία συνιστάται..

Το Snort αποτελεί μια από τις πιο μοντέρνες εφαρμογές στον τομέα της αναγνώρισης εισβολών, προσφέροντας 3 βασικές λειτουργίες. Μπορεί να λειτουργήσει: α) ως παρατηρητής πακέτων δικτύου (networkpacketsniffer), β) ως καταγραφέας δικτυακών πακέτων ή γ) ως ένα Network-based IDS. Υπάρχουν, επίσης, πάρα πολλά προγράμματα που μπορούν να προστεθούν στο Snort τα οποία προσφέρουν επιπλέον τρόπους διαχείρισης των αρχείων καταγραφών του (logfiles) και μπορούν να ανανεώνουν το σετ των υπογραφών/κανόνων της μηχανής ανίχνευσης. Με αυτό τον τρόπο, δίνεται η δυνατότητα στους διαχειριστές των δικτύων να ελέγξουν με πιο αποδοτικό τρόπο την πιθανότητα ύπαρξης κακόβουλης κίνησης και να μπορούν να ειδοποιηθούν σε αντίστοιχη περίπτωση.[8]

Τα βασικότερα στοιχεία που διατηρεί το Snort από την αρχή της υλοποίησής του (από τον MartinRoesch) μέχρι και σήμερα είναι ότι μπορεί να λειτουργήσει σε διάφορα λειτουργικά συστήματα και ότι πρόκειται για μια φορητή εφαρμογή. Τέλος, έχει έξοδο και σε δεκαεξαδική αλλά και σε ASCII μορφή, ενώ όλων των ειδών τα πακέτα μπορούν να αποτυπωθούν με μια πλήρη, σταθερή και συνεπή μορφή.

Τα δύο βασικά συστατικά του Snort είναι τα ακόλουθα:

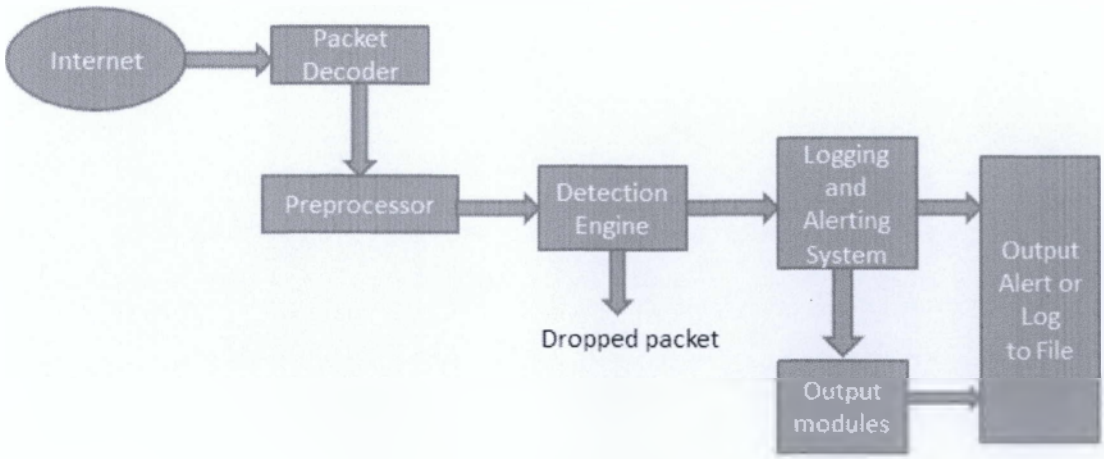
- Μηχανή ανίχνευσης που χρησιμοποιεί σπονδυλωτή αρχιτεκτονική plug-in.
- Ευέλικτη γλώσσα κανόνων για να περιγράψει την κυκλοφορία που πρέπει να συγκεντρωθεί.

2.2.2. Αρχιτεκτονική Snort

Το Snort επεξεργάζεται τα δεδομένα σε ένα νήμα (single-threaded) και σε πέντε στάδια. Στο πρώτο στάδιο γίνεται συλλογή των πακέτων τα οποία περνούν από τον αποκωδικοποιητή του Snort, ενώ με κατάλληλη ρύθμιση, μπορεί να γίνει και ανίχνευση επιθέσεων με τη χρήση των ειδοποιήσεων του αποκωδικοποιητή (decoderalerts). Στη συνέχεια ενεργοποιούνται όλοι οι προεπεξεργαστές, που πέρα από αποκωδικοποιήσεις και περαιτέρω επεξεργασία των πακέτων, μπορούν επίσης να ανιχνεύσουν επιθέσεις και να στείλουν ειδοποιήσεις. Πρόκειται για το σημείο που το Snort, αν και ανήκει στην κατηγορία των IDS υπογραφών, εισάγει με δικό του τρόπο την έννοια της ανίχνευσης ανωμαλιών. Έπειτα, ενεργοποιείται ο μηχανισμός ανίχνευσης επιθέσεων με εφαρμογή των υπογραφών/κανόνων του Snort στα επεξεργασμένα πακέτα. Τέλος, γίνονται γνωστά στο χρήστη τα αποτελέσματα της λειτουργίας του Snort από τις διαφορετικές μονάδες εξόδου.[8][9]

Τα στάδια από τα οποία απαρτίζεται το Snort είναι τα ακόλουθα:

- Αποκωδικοποιητής πακέτων (decoder).
- Οι Προεπεξεργαστές (preprocessors).
- Η Μηχανή Ανίχνευσης (detectionengine).
- Σύστημα καταγραφής και ειδοποιήσεων.
- Μονάδες Εξόδου (outputplugins).



Εικόνα 3: Αρχιτεκτονική Snort

Αποκωδικοποιητής πακέτων (decoder)

Ο αποκωδικοποιητής του Snort βασίζεται στην βιβλιοθήκη libpcap και υποστηρίζειένα μεγάλο αριθμό επιπέδων σύνδεσης όπως: Ethernet, 802.11, TokenRing, FDDI, CiscoHDLC, Slip, PPP, OpenBSDPF. Παίρνει τα πακέτα από διάφορους τύπους δικτύων (ενσύρματα και ασύρματα) και τα προετοιμάζει έτσι ώστε να μπορούν να επεξεργαστούν ή να σταλούν στη μηχανή ανίχνευσης. Η μηχανή αποκωδικοποίησης οργανώνεται γύρω από τα επίπεδα σύνδεσης του εκάστοτε συστήματος και τον τρόπο που έχουν οριστεί τα πρωτόκολλα TCP και IP. Κάθε υπορουτίνα του αποκωδικοποιητή δηλώνει τη σειρά των δεδομένων στο πακέτο και επικαλύπτει τις δομές της πρωταρχικής μορφής τους στο δίκτυο (rawpacketdata).

Οι Προεπεξεργαστές (preprocessors)

Οι προεπεξεργαστές είναι ανεξάρτητες μονάδες του Snort που μας επιτρέπουν να δούμε την εισερχόμενη πληροφορία με διαφορετικούς τρόπους προτού η μηχανή ανίχνευσης αναλάβει δράση για να ανιχνεύσει τυχόν επιθέσεις. Κάθε μονάδα αναπτύσσεται ως ξεχωριστό κομμάτι κώδικα στο δικό του ανεξάρτητο πηγαίο αρχείο. Η υλοποίηση τους ως ανεξάρτητα υποσυστήματα επιτρέπει σε κάποιον να επιλέξει ποιοι από αυτούς θα είναι ενεργοποιημένοι, προσαρμόζοντας το Snort στα δεδομένα και τις απαιτήσεις του εκάστοτε διαχειριστή και του εκάστοτε δικτύου. Κάθε προεπεξεργαστής εκκινεί με σειρά που έχει οριστεί στο αρχείο διαμόρφωσης (snort.conf).

Κάθε πακέτο περνάει από τους προεπεξεργαστές με τη σειρά που ορίσαμε στο αρχείο διαμόρφωσης, γι αυτό, η ενεργοποίηση τους πρέπει να γίνει με μια λογική σειρά. Αν τρέξουμε το Snort χωρίς προεπεξεργαστές, το μόνο πράγμα που βλέπουμε είναι τα πακέτα ως μονάδες/ανεξάρτητα πακέτα, όπως καθένα από αυτά μεταφέρθηκε από το υλικό του δικτύου (overthewire). Όμως, το πιο πιθανό είναι να χάσουμε επιθέσεις, καθώς πλέον είναι σύνηθες οι περισσότερες επιθέσεις να «κρύβονται», όπως γίνεται με επιθέσεις που μεταφέρουν τα δεδομένα τους σε επικαλυπτόμενα πακέτα που έχουν διασπαστεί (overlappingfragmentedpackets). Σε άλλες περιπτώσεις, χρησιμοποιείται η τεχνική της διαφυγής (evasionattacks) όπου μέρος της επίθεσης είναι σε ένα πακέτο και το υπόλοιπο σε κάποιο επόμενο.

Για να μπορεί να αναγνωρίζει τέτοιες επιθέσεις, το snort έχει προσαρμοστεί κατάλληλα ξεπερνώντας τα αυστηρά όρια ενός IDS κανόνων και υπογραφών. Ακόμα, μερικοί preprocessors σε ένα IDS έχουν και αυτοί τη δυνατότητα να ειδοποιήσουν τους διαχειριστές του συστήματος για τυχπόν επιθέσεις Οι προεπεξεργαστές είναι πολύ σημαντικοί για οποιαδήποτε IDS προκειμένου να προετοιμάσει τα πακέτα δεδομένων που προορίζονται για ανάλυση από τις μηχανές ανίχνευσης. Οι χάκερς χρησιμοποιούν διάφορες τεχνικές για να 'ξεγελάσουν' ένα IDS. Οι προεπεξεργαστές προσφέρουν τις εξής τρεις λειτουργίες: α) πραγματοποιούν δικούς τους ελέγχους με τη δυνατότητα να ενεργοποιήσουν ειδοποιήσεις, β) κανονικοποιούν τα δεδομένα ώστε να απλοποιήσουν τους κανόνες ανίχνευσης και γ) προσφέρουν νέους κανόνες.

Η Μηχανή Ανίχνευσης (detectionengine)

Η μηχανή ανίχνευσης του Snort είναι ίσως το αντιπροσωπευτικότερο κομμάτι λειτουργίας του ως NIDS. Είναι το μέρος που εισέρχεται η επεξεργασμένη πλέον από τους αποκωδικοποιητές και προεπεξεργαστές πληροφορία και συγκρίνεται με τους κανόνες του Snort. Η ευθύνη της είναι να ανιχνεύει εάν υπάρχει οποιαδήποτε εισβολή σε κάποιο από τα πακέτα του εξετάζει. Η μηχανή ανίχνευσης χρησιμοποιεί τους κανόνες του Snort για το λόγο αυτό. Οι κανόνες διαβάζονται σε εσωτερικές δομές δεδομένων και έπειτα σύμφωνα με αυτούς εξετάζονται τα πακέτα δεδομένων. Εάν ένα πακέτο ανταποκρίνεται στις απαιτήσεις κάποιου κανόνα, τότε η κατάλληλη ενέργεια λαμβάνεται για το πακέτο αυτό διαφορετικά 'αφήνεται ελεύθερο'. Μια από τις κατάλληλες ενέργειες είναι η ειδοποίηση του διαχειριστή τους συστήματος.

Η μηχανή ανίχνευσης είναι κρίσιμο κομμάτι του Snort. Ανάλογα με το πόσο ισχυρό είναι το υπολογιστικό σύστημα στο οποίο είναι εγκατεστημένο το Snort και ανάλογα με το πόσοι κανόνες έχουν καθοριστεί, διαφέρει και ο χρόνος επεξεργασίας των διαφόρων πακέτων που δέχεται το Snort για έλεγχο. Εάν η κυκλοφορία σε ένα δίκτυο είναι πάρα πολύ υψηλή όταν το Snort εργάζεται σε NIDSmode, τότε ο έλεγχος για τυχόν επιθέσεις ίσως να καθυστερήσει σημαντικά. Το 'φορτίο' στη μηχανή ανίχνευσης εξαρτάται από τους ακόλουθους παράγοντες:

- Αριθμός κανόνων.
- Επεξεργαστική ισχύς του συστήματος που είναι εγκατεστημένο στο Snort.

- Ταχύτητα των διαύλων του συστήματος του Snort.
- Το φορτίο του δικτύου.

Κατά το σχεδιασμό ενός συστήματος ανίχνευσης παρεισφρήσεων, όλοι οι παραπάνω παράγοντες θα πρέπει να λαμβάνονται υπόψη. Το σύστημα ανίχνευσης μπορεί να διασπάσει ένα πακέτο σε άλλα μικρότερα και να εφαρμόσει τους κανόνες στα διασπασμένα πλέον μέρη. Αυτά τα μέρη μπορεί να είναι:

- Η IP του πακέτου.
- Τα πρωτόκολλα TCP, ICMP ή σε άλλα πρωτόκολλα.
- Οι «επικεφαλίδες» της επιγραφής του DNS, τουFTP, της SNMP και του SMTP.

Συστήματα καταγραφής και ειδοποιήσεων

Ανάλογα με το τι εντοπίζει το σύστημα ανίχνευσης μέσε σε ένα πακέτο, το πακέτο ίσως να καταγράφει, ή εξαιτίας αυτού να ειδοποιηθεί ο διαχειριστής του συστήματος. Οι καταγραφές για τα συμβάντα που αντιμετωπίζει το Snort αποθηκεύονται σε μορφή απλών αρχείων κείμενων, αρχείων τύπου tcpdump-styleή σε κάποια άλλη μορφή. Όλα τα αρχεία αποθηκεύονται εξ ορισμού στον κατάλογο /var/log/. Μπορεί να γίνει αλλαγή της τοποθεσίας μέσω της γραμμής εντολών του Snort και της χρήσης εντολής-l.

Μονάδες εξόδου (outputplugins)

Αμέσως μετά τον έλεγχο της πληροφορίας με τους κανόνες, το Snort περνάει στη φάση της ειδοποίησης και καταγραφής. Κατά την καταγραφή των γεγονότων, το Snort κρατάει τα πακέτα που προξένησαν την ενεργοποίηση κανόνων, ενώ παράλληλα ειδοποιεί το χρήστη για το ποιος κανόνας ενεργοποιήθηκε ακριβώς. Όπως και με τους προεπεξεργαστές, πρόκειται για συναρτήσεις των οποίων η επιλογή και λειτουργία τίθεται στο αρχείο snort.conf. Οι μονάδες εξόδου έγιναν επιτρέπουν στο διαχειριστή να έχει μια πιο εύχρηστη δομή και παρουσίαση της πληροφορίας εξόδου από τη μηχανή του Snort.

Η ανάλυση των πακέτων και της πληροφορίας τους θα είχε τελείως άλλη μορφή, αν δεν υπήρχαν αυτές οι μονάδες που επεξεργάζονται και αποθηκεύουν τα δεδομένα. Βρίσκονται στο εσωτερικό του προγράμματος και προσφέρουν ένα ανοικτό API, ώστε να μπορεί κάποιος, ανεξάρτητα της ομάδας ανάπτυξης του Snort, να επέμβει και να προσαρμόσει τις πληροφορίες εξόδου στο δικό του περιβάλλον. Επίσης τα output modules μπορούν να κάνουν πράγματα όπως:

- Απλή καταγραφή στα αρχεία /var/log/snort/alerts ή σε κάποιο άλλο αρχείο.
- Αποστολή των SNMPtraps.
- Αποστολή μηνυμάτων στο syslog.
- Καταγραφή σε μια βάση δεδομένων όπως την MySQL ή Oracle.
- Παραγωγή αρχείων τύπου XML.
- Τροποποίηση των ρυθμίσεων στους δρομολογητές και τα firewalls.
- Αποστολή μηνυμάτων με την μορφή pop-upwindows σε windows-based συστήματα.
- Αποστολή ειδοποιήσεων σε μορφή e-mail.
- Αποστολή ειδοποιήσεων σε web-interfaces.
- Δομή του κανόνα του Snort

Υποστηριζόμενες πλατφόρμες

Το Snort υποστηρίζεται από μεγάλο μέρος λειτουργικών συστημάτων. Την τρέχουσα στιγμή το Snort είναι διαθέσιμα στα παρακάτω συστήματα:[22]

- Linux
- OpenBSD
- FreeBSD
- NetBSD
- Solaris (both Sparc and i386)
- HP-UX
- AIX
- IRIX
- MacOS
- Windows

2.2.3. Κανόνες Snort

Οι κανόνες του Snort υποδηλώνουν όχι μόνο τι θέλουμε να ψάξει το σύστημα στα εισερχόμενα πακέτα, αλλά και τι ενέργεια θέλουμε να εκτελέσει σε περίπτωση που βρεθεί πακέτο που να ικανοποιεί όλες τις συνθήκες του κανόνα. Σχεδόν όλοι οι κανόνες έχουν γραφτεί με στόχο την ανίχνευση και απαγόρευση διέλευσης σε πακέτα που περιέχουν «υπογραφές εισβολής» (intrusionsignatures),δηλαδή ορισμένα χαρακτηριστικά στοιχεία ενός συγκεκραμένου τύπου επίθεσης, τα οποία μπορεί να είναι καθορισμένοι παράμετροι στην επικεφαλίδα του πακέτου (packetheader) ή/και στα δεδομένα του πακέτου (payload). Τέτοιου είδους πακέτα συνήθως αποτελούν μέρος προσπάθειας που γίνεται με στόχο να πληγεί η ακεραιότητα του υπολογιστή του χρήστη και δεν θέλουμε να επιτραπεί η διέλευσή τους. Δίνεται, όμως, και η δυνατότητα συγγραφής κανόνων οι οποίοι έχουν ως στόχο να επιτρέπουν τη διέλευση πακέτων που πληρούν συγκεκριμένες προϋποθέσεις.

Οι κανόνες του Snort βρίσκονται κατηγοριοποιημένοι σε διάφορα αρχεία με κατάληξη ".rules", με το κάθε αρχείο να περιέχει, συνήθως, κανόνες που συμπεριλαμβάνονται σε ένα συγκεκριμένο τύπο επίθεσης απέναντι στο σύστημα. Για παράδειγμα, το αρχείο "ftp.rules" περιέχει κανόνες που είναι γραμμένοι με στόχο πακέτα που σχετίζονται με εφαρμογές ftp. Σε κάθε έκδοση του Snort που είναι διαθέσιμη στο δίκτυο συμπεριλαμβάνονται και συγκεκριμένα αρχεία κανόνων, ενώ ανά περιόδους γίνονται διαθέσιμα νέα αρχεία κανόνων ώστε να είναι εύκολος ο εκσυγχρονισμός του Snort απέναντι σε νέες μορφές επίθεσης. Επιπλέον, ο χρήστης μπορεί να επιλέγει ποια αρχεία κανόνων θέλει να χρησιμοποιούντα στο σύστημα του κάνοντας απλές τροποποιήσεις σε ένα αρχείο ρύθμισης (configuration) του Snort. Το σημαντικότερο, όμως, είναι πως ο χρήστης έχει τη δυνατότητα να γράφει νέους κανόνες, επιτρέποντας έτσι την προσαρμογή του Snort στις απαιτήσεις του κάθε χρήστη και στο είδος κίνησης που αναμένεται να υπάρχει στο συγκεκριμένο δίκτυο.

Το Snort χρησιμοποιεί μια απλή γλώσσα περιγραφής κανόνων η οποία όμως προσφέρει πληθώρα επιλογών που την κάνουν αρκετά ισχυρή και ευέλικτη. Υπάρχουν ορισμένες απλές αρχές που χρειάζεται να θυμάται κάποιος που ενδιαφέρεται να γράψει δικούς του κανόνες για το Snort. Οι περισσότεροι κανόνες γράφονται σε μια μόνο γραμμή. Σε εκδώσεις του Snort πριν από την 1.8 κάτι τέτοιο ήταν απαραίτητο, όμως στις νεότερες εκδόσεις είναι εφικτό να έχουμε κανόνες που

καταλαμβάνουν περισσότερο από μία γραμμή, αρκεί στο τέλος κάθε ενδιάμεσης γραμμής να βρίσκεται ο χαρακτήρας '\'. Όλοι οι κανόνες αποτελούνται από δύο λογικές ενότητες, την επικεφαλίδα του κανόνα (ruleheader) και τις ρυθμίσεις του κανόνα (ruleoption).

Στην επικεφαλίδα του κανόνα περιέχονται οι πληροφορίες για την ενέργεια που θα εκτελέσει το Snort σε περίπτωση που επαληθευτεί ο κανόνας, το πρωτόκολλο, οι διευθύνσεις IP του αποστολέα και του παραλήπτη μαζί με τις κατάλληλες μάσκες δικτύου (netmasks) καθώς και οι θύρες (ports) αποστολέα και παραλήπτη. Το τμήμα των ρυθμίσεων του κανόνα περιλαμβάνει τα μηνύματα προειδοποίησης (alerts) που θα παράγει το Snort σε περίπτωση επαλήθευσης καθώς και πληροφορίες για το ποια τμήματα του εισερχομένου πακέτου πρέπει να εξεταστούν ώστε να αποφασίσουμε αν το πακέτο είναι ύποπτο, οπότε το Snort θα δράσει κατάλληλα, ή όχι.

Ένας τυπικός κανόνας του Snort φαίνεται παρακάτω.

alerttcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg:"mountd

access";)

Οτιδήποτε πριν την πρώτη παρένθεση αποτελεί την επικεφαλίδα του κανόνα, ενώ το τμήμα μέσα στις παρενθέσεις αποτελεί τις ρυθμίσεις του κανόνα. Στο κομμάτι των ρυθμίσεων του κανόνα, οι λέξεις που βρίσκονται αμέσως πριν από ':' είναι οι εντολές ή λέξεις κλειδιά των ρυθμίσεων

Οι επικεφαλίδες των κανόνων

Η επικεφαλίδα κανόνων περιέχει τις πληροφορίες που καθορίζουν από πού έρχεται το ύποπτο πακέτο, που πηγαίνει και τι είδους είναι, καθώς επίσης και τι πρέπει να κάνουμε στην περίπτωση που μας έρθει ένα πακέτο με τα συγκεκριμένα χαρακτηριστικά του κανόνα. Το πρώτο στοιχείο σε κάθε κανόνα είναι η ενέργεια που θα εκτελεστεί (action), δηλαδή ο τρόπος που θα αντιδράσει το Snort σε περίπτωση που βρεθεί ένα πακέτο το οποίο ικανοποιεί όλα τα στοιχεία του κανόνα. Υπάρχουν οι εξής πέντε προκαθορισμένες ενέργειες στο Snort:

- alert – δημιουργία μηνύματος προειδοποίησης και καταγραφή του πακέτου.
- log – καταγραφή του πακέτου.

- pass – επιτρέπεται η διέλευση του πακέτου.
- activate – δημιουργία προειδοποίησης και ενεργοποίηση ενός dynamic κανόνα.
- dynamic – παραμένει ανενεργός μέχρι να επαληθευτεί ο αντίστοιχος activate κανόνας και μετά ενεργεί ως κανόνας τύπου log.

Το επόμενο πεδίο στην επικεφαλίδα ενός κανόνα είναι το πρωτόκολλο. Το Snort υποστηρίζει τέσσερα πρωτόκολλα στην ανάλυση εισερχομένων πακέτων, τα πρωτόκολλα tcp, udp, ip και icmp. Μετά το πρωτόκολλο βρίσκεται το τμήμα που περιέχει τις πληροφορίες για τις διευθύνσεις IP και τις θύρες του κανόνα.

Η λέξη-κλειδί 'any' μπορεί να χρησιμοποιηθεί όταν θέλουμε τον κανόνα να ισχύει για οποιαδήποτε διεύθυνση IP. Κάθε διεύθυνση αποτελείται από μία συνεχόμενη διεύθυνση IP (δηλαδή τέσσερις ακέραιους αριθμούς από 0 μέχρι 255 με '.' ανάμεσα τους) και ένα μπλοκ CIDR. Το μπλοκ CIDR το οποίο υποδηλώνει τη μάσκα δικτύου που εφαρμόζεται στην διεύθυνση κάθε πρώτου πακέτου γίνεται σύγκριση με τη διεύθυνση του κανόνα. Για παράδειγμα, ο συνδυασμός 192.168.1.0/24 υποδηλώνει την ομάδα διευθύνσεων από 192.168.1.0 μέχρι 192.168.1.255. Η χρήση του CIDR μας επιτρέπει να δηλώνουμε με ένα σύντομο τρόπο μεγάλες ομάδες διευθύνσεων. Εάν κάποιο εισερχόμενο πακέτο έχει τη διεύθυνσή του μέσα στο συγκεκριμένο πεδίο τιμών τότε επαληθεύεται αυτό το κομμάτι του κανόνα.

Στις διευθύνσεις μπορεί να εφαρμοστεί ένας τελεστής αντιστροφής, ο οποίος συμβολίζεται με '!' και λέει στο Snort ότι ταιριάζουν όλες οι διευθύνσεις εκτός από την αναγραφομένη. Για παράδειγμα, στην ακόλουθη επικεφαλίδα κανόνα δε μας ενδιαφέρει η διεύθυνση αποστολέα, καθώς είναι ρυθμισμένη σε any, και θέλουμε η διεύθυνση του παραλήπτη να μην ανήκει στην ομάδα 192.168.1.0/24.

alerttcpanyany -> !192.168.1.0/24 111 (...)

Το Snort υποστηρίζει μια ομάδα διευθύνσεων εσωκλείεται σε αγκύλες και κάθε διεύθυνση διαχωρίζεται από τις γειτονικές τις με ','. Δεν επιτρέπεται η ύπαρξη κενού (space). Για παράδειγμα, η έκφραση ' ![192.168.1.0/24,10.1.1.0/24] ' αναφέρεται για τις διευθύνσεις που δεν ανήκουν σε καμία από τις δύο ομάδες διευθύνσεων.

Το τελευταίο συστατικό της επικεφαλίδας ενός κανόνα είναι ο τελεστής κατεύθυνσης. Ο τελεστής αυτός βρίσκεται ανάμεσα στα δύο ζεύγη διεύθυνσης IP-θύρας και συμβολίζει την κατεύθυνση της κίνησης που μας ενδιαφέρει. Υπάρχει επίσης και ο αμφίδρομος τελεστής '<>' με τον οποίο δηλώνουμε ότι δε μας ενδιαφέρει ο προσανατολισμός της κίνησης. Για παράδειγμα, η χρήση αμφίδρομου τελεστή για την καταγραφή και των δύο πλευρών είναι ο εξής:

logtcp !192.168.1.0/24 any<> 192.168.1.0/24 23

Οι ρυθμίσεις (options) των κανόνων

Οι ρυθμίσεις των κανόνων του Snort συνδυάζουν ευκολία χρήσης, αποτελεσματικότητα και ευελιξία. Κάθε ρύθμιση σε έναν κανόνα διαχωρίζεται από την επόμενη με το χαρακτήρα ';'. Οι λέξεις-κλειδιά των ρυθμίσεων διαχωρίζονται από τα ορίσματά τους μέσω ':'. Οι ρυθμίσεις των κανόνων υπάγονται στις ακόλουθες τέσσερις κύριες κατηγορίες

Βοηθητικές: Παρέχουν επιπλέον πληροφορίες για τον κανόνα χωρίς, όμως, να σχετίζονται με την αναζήτηση.

Περιεχομένου: Όλες οι επιλογές του τύπου αυτού προσδιορίζουν δεδομένα που θα αναζητηθούν στο περιεχόμενο (payload) του πακέτου και μπορούν να συσχετίζονται μεταξύ τους.

Μη-περιεχομένου: Εξετάζουν πληροφορίες που δεν βρίσκονται στο περιεχόμενο

(payload) του πακέτου.

Ολοκληρωμένης αναζήτησης: Προσδιορίζουν την εκτέλεση ορισμένων γεγονότων που θα συμβούν όταν επαληθευτεί ο κανόνας.[10]

2.2.4. Η τυπική επεξεργασία κανόνων στο Snort

Το Snort χρησιμοποιεί τις παραμέτρους των πρωτοκόλλων για να διαχωρίζει τους κανόνες σε ξεχωριστές ομάδες. Στις παλιότερες εκδόσεις του Snort, χρησιμοποιούνταν μια καθαρά παραμετρική αναζήτηση για να εξετάζεται κατά πόσο ένα πακέτο ικανοποιεί τις παραμέτρους μίας ομάδας κανόνων. Οι κανόνες

κατατάσσονταν σε διαφορετικές ομάδες με βάση τέσσερα γενικά χαρακτηριστικά, τέσσερις βασικές παραμέτρους:

- Η διεύθυνση IP του αποστολέα.
- Η διεύθυνση IP του παραλήπτη.
- Οι πιθανές τιμές για τη θύρα του αποστολέα.
- Οι πιθανές τιμές για τη θύρα του παραλήπτη.

Όταν εξεταζόταν ένα πακέτο, γινόταν έλεγχος κατά πόσο ταιριάζει με αυτές τις τέσσερις παραμέτρους κάθε ομάδας κανόνων. Εάν το πακέτο δεν ταίριαζε και στις παραμέτρους μίας ομάδας τότε ο έλεγχος προχωρούσε στην επόμενη ομάδα κανόνων. Σε περίπτωση που το πακέτο ικανοποιούσε όλες τις παραμέτρους τότε όλοι οι κανόνες μέσα στην ομάδα εξετάζονταν διαδοχικά και οι υπόλοιποι παράμετροι κάθε κανόνα εξετάζονταν κατά σειρά. Μόλις ολοκληρωνόταν η αναζήτηση όλων των κανόνων σε μία ομάδα, οι τέσσερις βασικές παράμετροι του πακέτου εξετάζονταν με αυτούς της επόμενης ομάδας κανόνων και η διαδικασία επαναλαμβανόταν.

Η διαδικασία αυτή είναι αποδοτική μόνο σε περίπτωση που έχουμε ένα μικρό αριθμό κανόνων. Εάν, για παράδειγμα, υπάρχουν περισσότεροι από 10 κανόνες σε κάθε ομάδα τότε η μέθοδος αυτή είναι αρκετά χρονοβόρα, καθώς οι κανόνες εξετάζονται διαδοχικά και όλοι οι παράμετροι κάθε κανόνα πρέπει να εξεταστούν ανεξάρτητα. Προκειμένου να βελτιωθεί η ταχύτητα επεξεργασίας των κανόνων, ήταν απαραίτητη η υλοποίηση μεθόδων ομαδικής επεξεργασίας.[10]

2.2.5. Διαδικασία ανίχνευσης του Snort

Το Snort έχει δύο κύριους τρόπους λειτουργίας. Η πρώτη είναι μια λειτουργία packetsniffer, το οποίο είναι παρόμοιο με το tcpdump. Τα πακέτα αποθηκεύονται σε ένα αρχείο καταγραφής, το οποίο επιτρέπει την μετέπειτα ανάλυση. Ο άλλος τρόπος λειτουργίας είναι ένα NetworkIntrusionDetectionSystem (NIDS). Όταν το λειτουργικό Snort είναι σε αυτή την κατάσταση, τα σύνολα κανόνων που εφαρμόζονται σε πακέτα, ψάχνουν για ύποπτη συμπεριφορά. Και οι δύο τρόποι λειτουργίας περιγράφονται παρακάτω.

PacketSniffer

Ο τρόπος με τον οποίο τρέχει το Snort σε ένα packetsniffer επιτρέπει στους διαχειριστές του συστήματος τη συλλογή και την αποθήκευση δεδομένων πακέτου. Το Snort μπορεί να ρυθμιστεί για να συλλέξει τα δεδομένα πακέτου σε διαφορετική λεπτομέρεια, ανάλογα με το πόσο είναι απαραίτητη η λεπτομέρεια. Αν και είναι παρόμοιο με το tcpdump, το Snort δεν έχει χαρακτηριστικά που εκτείνονται πέρα από την ικανότητα του tcpdump. Το κύριο χαρακτηριστικό που έχει το Snort με το tcpdump δεν είναι το πακέτο ελέγχου ωφέλιμου φορτίου. Το Snort αποκωδικοποιεί το στρώμα εφαρμογής ενός πακέτου και μπορεί να δοθεί

alertip any any -> any any (msg: "IP Packet detected";)

Σε αυτό το παράδειγμα, μια ειδοποίηση παράγεται κάθε φορά ως πακέτο IP και ανιχνεύεται, είτε από την αποστολή είτε από τη λήψη.

NetworkIntrusionDetectionMode

Ο τρόπος με τον οποίο τρέχει το Snort σε λειτουργία ανίχνευσης εισβολέων είναι εντελώς διαφορετική από ό, τι τρέχει στο πακέτο sniffermode. Το δίκτυο ανίχνευσης εισβολών δεν συλλαμβάνει/καταγράφει τα πακέτα δικτύου. Αντ 'αυτού, εφαρμόζει ένα σύνολο κανόνων σχετικά με κάθε πακέτο που περνάει. Το σύνολο των κανόνων διαχειρίζονται από το διαχειριστή του συστήματος και θα πρέπει να αντανακλούν κοινά πρότυπα εισβολής.

Αυτά τα πρότυπα είναι πολλά όπως τα αρχεία ορισμού ιών στο ότι δείχνουν μια λίστα με κοινά πρότυπα πακέτων που δείχνουν γενικά μια εισβολή ή κατάχρηση του συστήματος. Δεν λαμβάνονται μέτρα εάν το πακέτο δεν ανταποκρίνεται σε έναν από τους κανόνες που εφαρμόζονται. Εάν ένα πακέτο δεν ταιριάζει με έναν από τους κανόνες, τότε το πακέτο είναι καταγραμμένο, και μπορεί επίσης να δημιουργήσει μια ειδοποίηση. Μια ειδοποίηση ενημερώνει τον διαχειριστή του συστήματος ότι μια αμφισβητήσιμο πακέτο έχει μόλις ληφθεί (ή σταλθεί) από ένα συγκεκριμένο σύστημα.

2.3. Εισαγωγή στο Bro

Το Bro είναι ένα σύστημα ανίχνευσης εισβολής που λειτουργεί παθητικά βλέποντας την κυκλοφορία σε μια σύνδεση δικτύου. Είναι χτισμένο γύρω από μια μηχανή ώστε τα κομμάτια πακέτων δικτύου να αντανακλούν σε διαφορετικά είδη δραστηριοτήτων. Μερικά γεγονότα είναι αρκετά χαμηλού επιπέδου, όπως η οθόνη να δει μια προσπάθεια σύνδεσης. Μερικά είναι ειδικά για ένα συγκεκριμένο πρωτόκολλο δικτύου, όπως ένα FTP. Και μερικοί εκφράζουν αρκετού υψηλού επιπέδου έννοιες, όπως ένας χρήστης που έχει πιστοποιηθεί με επιτυχία κατά τη διάρκεια μιας περιόδου σύνδεσης.

Bro είναι ένα Unix-based σύστημα ανίχνευσης εισβολών (IDS). Το σύστημα Bro παρακολουθεί την κίνηση στο δίκτυο και ανιχνεύει απόπειρες εισβολής με βάση τα χαρακτηριστικά της κυκλοφορίας και το περιεχόμενο. Το σύστημα Bro ανιχνεύει εισβολές από τη σύγκριση της κίνησης δικτύου κατά τους κανόνες που περιγράφουν τα γεγονότα, που κρίνονται ενοχλητικά. Οι κανόνες αυτοί μπορούν να περιγράψουν τις δραστηριότητες (π.χ., certainhosts σύνδεση με ορισμένες υπηρεσίες), ποιες δραστηριότητες αξίζουν προειδοποίησης (π.χ., προσπαθεί σε ένα δεδομένο αριθμό διαφορετικών hosts να γίνει "σάρωση"), ή υπογραφές που περιγράφουν γνωστές επιθέσεις ή την πρόσβαση σε γνωστά τρωτά σημεία.

Αν το σύστημα Bro εντοπίσει κάτι ενδιαφέρον, μπορεί να διαταχθεί να εκδίδουν είτε μια καταχώρηση στο μητρώο ή να ξεκινήσει την εκτέλεση μίας εντολής του λειτουργικού συστήματος. Το σύστημα Bro στοχεύει στην υψηλή ταχύτητας (Gbit / s), στον υψηλό όγκο ανίχνευσης εισβολής. Με τεχνικές φιλτραρίσματος, το σύστημα Bro είναι σε θέση να επιτύχει την απαραίτητη απόδοση για να το πράξουν, ενώ λειτουργεί με εμπορικό διαθέσιμο υλικό του υπολογιστή και, συνεπώς, μπορεί να χρησιμεύσει ως ένα αποτελεσματικό μέσο κόστος της παρακολούθησης σύνδεση στο Internet.[28]

2.3.1. Τι είναι το Bro

Το σύστημα Bro είναι ένα open-source, Unix-based σύστημα ανίχνευσης εισβολών (IDS) που παρακολουθεί παθητικά την κυκλοφορία του δικτύου και ψάχνει για ύποπτη δραστηριότητα. Το σύστημα Bro ανιχνεύει εισβολές από την πρώτη

κυκλοφορία του δικτύου ανάλυσης για να εξαγάγετε σε επίπεδο εφαρμογής και μετά την εκτέλεση σε αναλυτές που συγκρίνουν τη δραστηριότητα με τα πρότυπα που κρίνονται ενοχλητικά.

Η ανάλυση περιλαμβάνει την ανίχνευση των ειδικών επιθέσεων συμπεριλαμβανομένων αυτών που ορίζονται από υπογραφές, αλλά και εκείνες που καθορίζονται από την άποψη των γεγονότων και τις ασυνήθιστες δραστηριότητες (π.χ. ορισμένες φιλοξενούν τη σύνδεση με ορισμένες υπηρεσίες ή πρότυπα με αποτυχημένες προσπάθειες σύνδεσης). Το Bro χρησιμοποιεί μια εξειδικευμένη γλώσσα της πολιτικής που επιτρέπει σε ένα site να χρησιμοποιεί τη λειτουργία tailor Bro, για αυτό οι πολιτικές ιστοσελίδες εξελίσσονται καθώς ανακαλύπτονται νέες επιθέσεις.

Αν το Bro εντοπίσει κάτι ενδιαφέρον, μπορεί να διαταχθεί είτε για να δημιουργήσει μια καταχώρηση στο μητρώο, να προειδοποίηση τον χειριστή σε πραγματικό χρόνο, να εκτελέσει μια εντολή του λειτουργικού συστήματος (π.χ., για να τερματίσει μια σχέση ή να εμποδίσουν ένα κακόβουλο υποδοχής on-the-fly). Επιπλέον, τα λεπτομερή αρχεία καταγραφής Bro μπορεί να είναι ιδιαίτερα χρήσιμα για την εγκληματολογία.[29]

2.3.2. Στόχος σχεδιασμού Bro

Ο σχεδιασμός του Bro καθοδηγείται από ένα σύνολο στόχων. Οι πιο σημαντικές από αυτές είναι:

Διαχωρισμός του μηχανισμού και της πολιτικής

Μια πολιτική ασφάλειας του δικτύου εξαρτάται σε μεγάλο βαθμό από συγκεκριμένο περιβάλλον. Για παράδειγμα, ενώ ένα δημόσιο ερευνητικό ινστιτούτο μπορεί συχνά να παρέχει πλήρης πρόσβαση στο Διαδίκτυο σε όλα τα συστήματα εσωτερικού, σε ένα εταιρικό δίκτυο μπορεί να χρειαστεί να επιβάλει σοβαρούς περιορισμούς. Με σαφή διαχωρισμό των μηχανισμών που απαιτούνται για την παρακολούθηση (και, ενδεχομένως, να επιβάλει) μια συγκεκριμένη ειδικευμένη πολιτική, κερδίζουμε τόσο την απλότητα όσο και την ευελιξία

Υψηλής ταχύτητας, μεγάλης παρακολούθησης του όγκου

Με το δίκτυο όπου το εύρος ζώνης φθάνει συνήθως ένα Gbit / s αυτές τις μέρες, κάθε NIDS πρέπει να είναι ιδιαίτερα αποτελεσματικό για την αντιμετώπιση αυτών των ποσών των δεδομένων σε πραγματικό χρόνο. Κάθε πακέτο μπορεί να πέσει δυνητικά να οδηγήσει σε μια χαμένη επίθεση.

Αντικρουόμενες επιθέσεις

Αν και δεν είναι συνήθως ο κύριος στόχος ενός εισβολέα να θέσει σε κίνδυνο ένα NIDS, είναι ένα προφανές πρώτο βήμα της επίθεσης για να απενεργοποιήσετε το NIDS πριν στοχεύσει στο πραγματικό θύμα. Ως εκ τούτου, ένα NIDS μπορεί να απενεργοποιηθεί εύκολα για αυτό δεν χρησιμοποιείτε.[12]

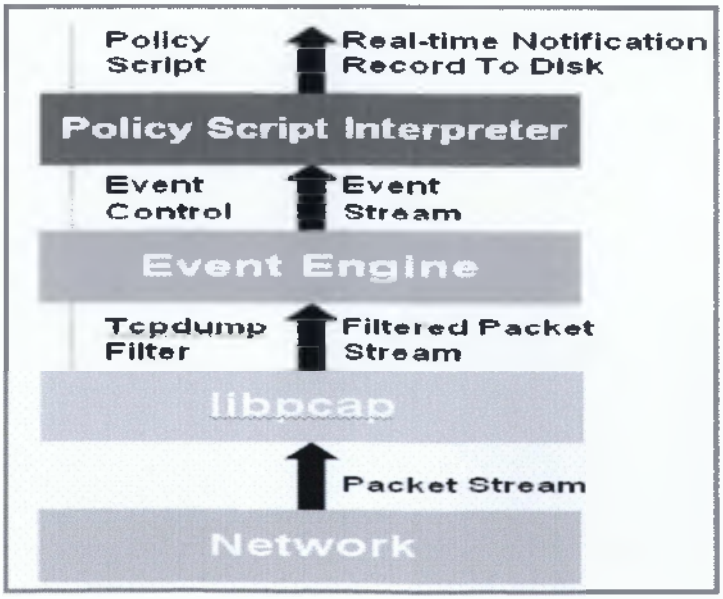
2.3.3. Αρχιτεκτονική του Bro

Αρχιτεκτονικά, το Bro επιστρώνεται σε τρία βασικά συστατικά, όπως φαίνεται στο σχήμα. Χρησιμοποιεί το πρότυπο libpcap πακέτων σύλληψης βιβλιοθήκης για να φιλτράρει τη ροή πακέτων. Τα φιλτραρισμένα πακέτα στη συνέχεια περνάνε μαζί στο Bro κινητήρα, η οποία μειώνει το φιλτραρισμένο ρεύμα σε μία σειρά γεγονότων σε υψηλότερο επίπεδο. Τα γεγονότα αυτά αντανακλούν τη δραστηριότητα του δικτύου στην πολιτική-ουδέτερο.

- Network: Τα χαμηλότερα στρώματα επεξεργάζονται το μεγαλύτερο όγκο των δεδομένων, και ως εκ τούτου πρέπει να περιορίσουν την εργασία που εκτελείται σε ένα ελάχιστο. Όπως πάμε ψηλά μέσα από τα στρώματα, τα δεδομένα μειώνονται, επιτρέποντας μεγαλύτερη επεξεργασία ανά είδος δεδομένων.
- Libpcap: Ακριβώς πάνω από το δίκτυο είναι το libpcap, το πακέτο-σύλληψη βιβλιοθήκη που χρησιμοποιείται από το tcpdump. Χρησιμοποιώντας τους στόχους του libpcap έχουμε σημαντικά πλεονεκτήματα: απομονώνεται το Bro από λεπτομέρειες του δικτύου τεχνολογίας σύνδεσης. Αν το λειτουργικό σύστημα υποδοχής παρέχει ένα αρκετά ισχυρό φίλτρο πακέτων πυρήνα, τότε το libpcap κατεβάζει το φίλτρο που χρησιμοποιείται για τη μείωση της κυκλοφορίας μέσα στον πυρήνα. Το κλειδί για την μεταφορά πακέτων φιλτραρίσματος είναι, φυσικά, η συνετή επιλογή ποια πακέτα θα κρατήσει και ποια θα απορρίψει.

- Eventengine: Το φιλτραρισμένο ρεύμα πακέτων στη συνέχεια παραδόθηκε μέχρι το επόμενο στρώμα, το Bro "μηχανή γεγονός." Αυτό το στρώμα εκτελεί για πρώτη φορά πολλούς ελέγχους ακεραιότητας για να εξασφαλίσει ότι οι επικεφαλίδες των πακέτων είναι καλοσχηματισμένες, όπως τον έλεγχο της κεφαλίδας IP checksum. Εάν αποτύχουν οι έλεγχοι αυτοί, τότε το Bro δημιουργεί ένα γεγονός που δείχνει το πρόβλημα και απορρίπτει το πακέτο. Είναι, επίσης, σε αυτό το σημείο ότι το Bro επανασυνδέει τα IP κομμάτια έτσι ώστε να μπορεί να τα αναλύσει στη συνέχεια. Εάν οι έλεγχοι επιτύχουν, τότε η μηχανή εκδήλωση αναζητά την κατάσταση σύνδεσης που συνδέονται με την πλειάδα των δύο διευθύνσεων IP και τα δύο TCP ή UDP αριθμούς θυρών. Στην συνέχεια, αποστέλλει το πακέτο σε ένα χειριστή για την αντίστοιχη σύνδεση.
- Policyscriptinterpreter:

Αφού ο κινητήρας ολοκληρώσει την επεξεργασία ενός πακέτου, τότε ελέγχει αν η επεξεργασία παράγει κάποιο γεγονός. Αυτό επεξεργάζεται κάθε περίπτωση μέχρι η ουρά να είναι άδεια. Επίσης ελέγχει αν κάποιο χρονόμετρο του γεγονός έχει λήξει, και αν τα επεξεργάζεται. Ένα βασικό γεγονός του σχεδιασμού Bro είναι η σαφής διάκριση μεταξύ των παραγόμενων γεγονότων σε σχέση με το τι πρέπει να κάνουμε σε ανταπόκριση με τα γεγονότα. Αυτή η δομή αντανακλά το διαχωρισμό μεταξύ του μηχανισμού και της πολιτικής.[11]



Εικόνα 4: Αρχιτεκτονική Bro

2.3.4. Χαρακτηριστικά των NIDS Bro

Το σύστημα Bro είναι ένα αυτόνομο σύστημα που χρησιμοποιείται για την ανίχνευση εισβολέων του δικτύου σε πραγματικό χρόνο με την παθητική παρακολούθηση της σύνδεση του δικτύου. Το σύστημα Bro παρέχει ένα σύνολο χαρακτηριστικών που το καθιστούν ένα ισχυρό σύστημα ανίχνευσης εισβολών.

Networkbased

Το σύστημα Bro είναι ένα δίκτυο που βασίζεται στο IDS. Συλλέγει φίλτρα και αναλύει την κυκλοφορία που περνά μέσα από μια συγκεκριμένη θέση του δικτύου. Μια ενιαία οθόνη Bro, στρατηγικά τοποθετημένα σε ένα βασικό δίκτυο συνδεσης, μπορεί να χρησιμοποιηθεί για την παρακολούθηση όλης της εισερχόμενης και εξερχόμενης κίνησης για ολόκληρο ιστό. Το σύστημα Bro δεν χρησιμοποιεί ή απαιτεί την εγκατάσταση του λογισμικού client σε κάθε δικτυωμένο ηλεκτρονικό υπολογιστή.

Richapplication-layeranalysis

Ένα κύριο χαρακτηριστικό του Bro είναι ότι περιλαμβάνει λεπτομερείς, με γνώμονα την ανάλυση των πολλών δημοφιλών πρωτοκόλλων εφαρμογής. Η παραγωγή αυτών των αναλυτών είναι ένα ρεύμα των γεγονότων που περιγράφουν την παρατηρούμενη δραστηριότητα σημασιολογικά, με υψηλού επιπέδου όρους. Αυτά τα ίδια τα γεγονότα δεν αποτελούν προειδοποιήσεις ασφαλείας, αλλά παρέχουν τα στοιχεία για περαιτέρω επεξεργασία χρησιμοποιώντας έθιμο γλώσσα του Bro.

Customscriptinglanguage

Σενάρια πολιτικής του Bro τα οποία είναι προγράμματα είναι γραμμένα στη γλώσσα του Bro. Περιέχουν όλους τους "κανόνες" που περιγράφουν ποια είναι τα είδη των δραστηριοτήτων που κρίνονται ενοχλητικά. Αναλύουν τη δραστηριότητα του δικτύου και ξεκινάει ενέργειες με βάση την ανάλυση. Παρόλο ότι η γλώσσα Bro παίρνει κάποιο χρόνο και προσπάθεια για να μαθευτεί, μόλις κατακτηθεί, ο χρήστης Bro μπορεί να γράψει ή να τροποποιήσει τις πολιτικές Bro να εντοπίσει και να ειδοποιεί σε σχεδόν οποιοδήποτε τύπο της δραστηριότητας του δικτύου.

Networktrafficanalysis

Το σύστημα Bro δεν εξετάζει μόνο για υπογραφές, αλλά επίσης αναλύει τα πρωτόκολλα δικτύου, τις συνδέσεις, τα δεδομένα και πολλά άλλα χαρακτηριστικά του δικτύου. Έχει ισχυρές εγκαταστάσεις για την αποθήκευση πληροφοριών σχετικά με το παρελθόν της δραστηριότητας και την ενσωμάτωσή της σε αναλύσεις σε νέες δραστηριότητες.

2.4. Σύγκριση του Bro και του Snort IDS

Το Snort παρέχει μια πολύ καλή ενημέρωση, καλά τεκμηριωμένο και δοκιμασμένο σύνολο κανόνων αλλά βρέθηκε ότι όσο ο αριθμός της υπογραφής αυξάνεται, η χρήση της Snort CPU και η χρήση της μνήμης αυξάνεται. Για να ξεπεραστεί αυτό το πρόβλημα του Snort, το Bro παρέχει μια ολοκλήρωμένη διαφορετική αρχιτεκτονική. Το μεγάλο χαρακτηριστικό γνώρισμα του Bro είναι ότι μπορεί να απομνημονεύει την κατάσταση της κάθε ροής, και να το χρησιμοποιήσει για ανίχνευση κακόβουλων δραστηριοτήτων. Παρά το γεγονός ότι έχουν πολλές διαφορές, και οι δύο είναι προσανατολισμένες προς την κατεύθυνση σύνδεσης υψηλής ταχύτητας.[13][14]

Snort IDS	Bro IDS
Μην χρησιμοποιείτε πολυεπίπεδη προσέγγιση.	Χρησιμοποιήστε Πολυεπίπεδη προσέγγιση.
Κανόνα κινητήρα αντιστοίχιση είναι πιο αποτελεσματική.	Λιγότερο αποτελεσματική από ό, τι το Snort.
Για την ανίχνευση εισβολών, οι υπογραφές είναι γραμμένα.	Να ορίζονται οι κανόνες πολιτικής.

Απόδοση υποβαθμίζει τον αριθμό των υπογραφών αυξήσεις.	Επιδόσεις δεν υποβαθμίζονται.
Ένα πολύ υψηλό πακέτων λείπει.	Το Bro περιλαμβάνει τόσο την υπογραφή αντιστοιχία του κινητήρα και μια εφαρμογή ανάλυσης scripting γλώσσας.
Εξαιρετικά τεκμηριωμένη.	Λιγότερη τεκμηρίωση

ΚΕΦΑΛΑΙΟ 3:Συστήματα πρόληψης εισβολών

3.1. Ορισμός IPS

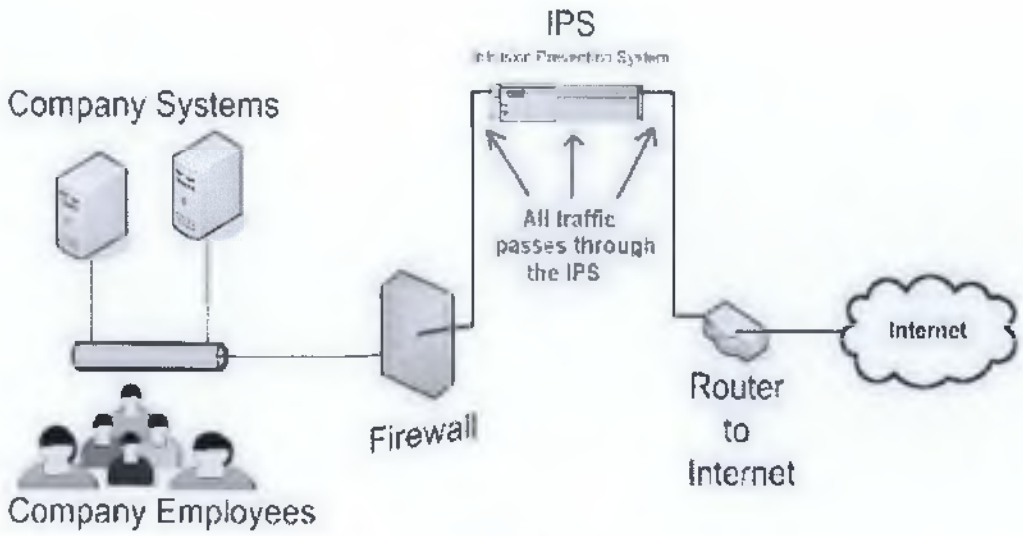
Συστήματα αποτροπής εισβολών (IPS), επίσης γνωστό ως πρόληψης συστημάτων, είναι συσκευές ασφάλειας του δικτύου που παρακολουθούν το δίκτυο ή το σύστημα

δραστηριοτήτων για κακόβουλη δραστηριότητα. Τα συστήματα IPS είναι μια τεχνολογία που χρησιμοποιούνται για την ανίχνευση και την πρόληψη ύποπτης κακόβουλης κίνησης του δικτύου ή τη συμπεριφορά του. Οι κύριες λειτουργίες των συστημάτων πρόληψης εισβολής είναι να προσδιορίσουν την κακόβουλη δραστηριότητα, να καταγράψουν πληροφορίες σχετικά με τη δραστηριότητα αυτή, και να προσπαθήσουν να την εμποδίσουν ή να την σταματήσουν.

Τα συστήματα πρόληψης εισβολών θεωρούνται επεκτάσεις των συστημάτων ανίχνευσης εισβολής, επειδή και οι δύο παρακολουθούν την κίνηση στο δίκτυο ή το σύστημα δραστηριοτήτων για κακόβουλη δραστηριότητα. Τα συστήματα IPS είναι συσκευές οι οποίες έχουν εγκατασταθεί σε κρίσιμα σημεία του δικτύου, για την εκτέλεση σε πραγματικό χρόνο ανάλυση της κίνησης του δικτύου. Οι κύριες διαφορές, σε αντίθεση με τα συστήματα ανίχνευσης εισβολής, τα συστήματα πρόληψης εισβολών τοποθετούνται σε σειρά και είναι σε θέση να συμμετάσχουν ενεργά στην πρόληψη και να μπλοκάρουν εισβολές που εντοπίζονται. Πιο συγκεκριμένα, η IPS μπορεί να πάρει τέτοιες ενέργειες, όπως η αποστολή συναγερμού, ρίχνοντας τα κακόβουλα πακέτα, να γίνει επαναφορά της σύνδεσης ή να παρεμποδίσει την κυκλοφορία από παραβίαση διεύθυνσης IP. [26]

Ένα σύστημα IPS, χρησιμοποιείται στην ασφάλεια των υπολογιστών. Παρέχει τις πολιτικές και τους κανόνες για την κυκλοφορία του δικτύου, μαζί με ένα σύστημα ανίχνευσης εισβολής για σύστημα συναγερμού ή διαχειρίσεις δικτύου για ύποπτη κίνηση, αλλά επιτρέπει στον διαχειριστή να παρέχει την ενέργεια μόλις ειδοποιηθεί.

Ένα σύστημα πρόληψης εισβολέων είναι ουσιαστικά μια επόμενη γενιά 'firewal' που συνδυάζει επίπεδο δικτύου και επίπεδο εφαρμογής τεχνικής φιλτραρίσματος σε συνδυασμό με ένα δραστικό σύστημα ανίχνευσης εισβολής (IDS) για να προστατεύσει προληπτικά μια συσκευή δικτύου ή προορισμού με βάση heuristics, ή το δίκτυο ανάλυσης της συμπεριφοράς . Μια IPS χρησιμοποιεί έλεγχο των πακέτων δεδομένων για να ξεπεραστούν οι αδυναμίες που αρχικά υπήρχαν εντός firewalls και IDS. Μια IPS είναι λιγότερο προϊόν παρά μια διαδικασία ή λειτουργία που είναι πλέον ενσωματωμένη μέσα σε μια ηλεκτρονική συσκευή ασφαλείας.[31]



Εικόνα 5: Λειτουργία IPS

Πρόληψη εισβολών θα πρέπει να θεωρηθεί ως μια προληπτική προαγοραστική προσέγγιση για την ασφάλεια του δικτύου που χρησιμοποιείται για τον εντοπισμό δυνητικών απειλών. Όπως ένα IDS, ένα IPS θα παρακολουθεί την κυκλοφορία του δικτύου για απειλές της ασφάλεια.

Στην απλούστερη έννοια, ένα σύστημα πρόληψης εισβολής είναι ένα in-line σύστημα που μπλοκάρει τις επιθέσεις για να μπορέσουν να φτάσουν το στόχο τους. Υπό μια ευρύτερη έννοια, η IPS εκτελεί μια βαθιά εξέταση των πακέτων, και ως εκ τούτου είναι σε θέση να επεκτείνει μια νέα σειρά από λειτουργίες που οφείλονται σε αυτή την ενδελεχή ανάλυση και ταξινόμηση της κίνησης.

3.1.1. Πλεονεκτήματα των IPS

Δεν υπάρχει αμφιβολία ότι ένα σύστημα πρόληψης είναι εξαιρετικά σημαντικό για τη διατήρηση της ασφάλειας του δικτύου από κακόβουλες δραστηριότητες. Ένα από τα μεγαλύτερα πλεονεκτήματα των IPS είναι ότι προστατεύει την κλοπή της πνευματικής ιδιοκτησίας εμποδίζοντας την ανεπιθύμητη πρόσβαση κακόβουλων δραστηριοτήτων. Επίσης μειώνει το χρόνο μη λειτουργίας και την φθορά για τα επιχειρησιακά συστήματα και των ιστοσελίδων από DDos επιθέσεις και απειλές. [33]

3.1.2. Βασικοί τύποι συστήματος IPS

Υπάρχουν διάφοροι τύποι των συστημάτων πρόληψης εισβολής, ανάλογα με το πού κατοικούν και τι προστατεύουν. Σε πολλές περιπτώσεις, οι συσκευές αυτές ενσωματώνονται με άλλες λειτουργίες όπως firewalls, ή με συστήματα ανίχνευσης εισβολών. Υπάρχουν τρεις βασικοί τύποι συστήματος IPS. Το Host-Based Intrusion Prevention Systems (HIPS), το Network Intrusion Prevention Systems (NIPS) και το Wireless Intrusion Prevention Systems.[32][34][35][36][37][38]

Host-Based Intrusion Prevention Systems (HIPS)

Host συστήματος αποτροπής εισβολών (HIPS) παρακολουθεί μια ενιαία υποδοχή για ύποπτη δραστηριότητα με την ανάλυση των γεγονότων που συμβαίνουν μέσα στον ξενιστή. Υπάρχουν λύσεις του HIPS για την προστασία του ξενιστή από το στρώμα του δικτύου σε όλη τη διαδρομή μέχρι το επίπεδο εφαρμογών από γνωστές και άγνωστες κακόβουλες επιθέσεις. Σε περίπτωση απόπειρας λειτουργικού συστήματος ή αλλαγές στην εφαρμογή από έναν χάκερ ή κακόβουλο λογισμικό, το HIPS αναστέλλει τη δράση και ενημερώνει το χρήστη με μια κατάλληλη απόφαση για τα επόμενα βήματα που μπορούν να γίνουν.

Αν και οι πωλητές των anti-virus και firewall αλλάζουν τον τρόπο που σαρώσουν την κάλυψη των αυξανόμενων αριθμών απειλών, και οι δύο είναι πάρα πολύ συχνά αντιδραστική. Αν γίνει η επίθεση προσπαθούν να εκμεταλλευτούν μια άγνωστη ευπάθεια, όμως η anti-virus δεν θα σταματήσει αν δεν έχει την υπογραφή για αυτό. Το HIPS θα λάβει μια διαφορετική προσέγγιση για την προστασία του υπολογιστή από τα παραδοσιακά anti-malware. ΤοHIPS παίρνει τον έλεγχο της ακεραιότητας της εφαρμογής αντί να προσπαθεί να ταιριάξει με υπογραφές ανάμεσα στα εκατομμύρια των malware παραδείγματα εκεί έξω.

Ένα HIPS σύστημα σαρώνει την κυκλοφορία, τόσο εξερχομένων όσο και εισερχομένων, σε μια δεδομένη υποδοχή. Αυτό το είδος της IPS έχει εγκατασταθεί ως λογισμικό σε έναν ξενιστή. Τρέχει ως διαδικασία και σαρώνει διάφορα χαρακτηριστικά του συστήματος υποδοχής (εκτελέσιμα, συνδέσεις και πρόσβαση σε αρχεία) και αποτρέπει κακόβουλες απόπειρες εισβολής.

Ένα IPS έχει εγκατασταθεί σε έναν κεντρικό υπολογιστή που είναι γνωστό ως πράκτορας. Ο πράκτορας σαρώνει τα χαρακτηριστικά υποδοχής και λαμβάνει προληπτικές δράσεις. Κάθε παράγοντας μεταδίδει τα δεδομένα ή τις πληροφορίες καταγραφής σε κεντρικούς εξυπηρετητές οι οποίοι χρησιμοποιούνται για τη διαχείριση πλήθους. Με αυτό τον τρόπο, κάθε πλήθος έχει τη δική του IPS, ενώ οι πληροφορίες για το πλήρες δίκτυο μπορεί να έχουν πρόσβαση μέσω της κεντρικής διαχείρισης των servers.

Μερικές φορές, ο παράγων τρέχει σε ατομικό ξενιστή που έχει ρυθμιστεί με τέτοιο τρόπο ώστε μια επίθεση να ανιχνεύεται από τον παράγοντα που αναφέρεται πίσω στον κεντρικό server. Ο κεντρικός υπολογιστής στέλνει την εντολή ελέγχου πίσω στον πράκτορα για να γνωρίζει ποια προληπτικά μέτρα πρέπει να ληφθούν. Αν και δεν υπάρχει τίποτα λάθος σε αυτό το είδος της ρύθμισης, η προσέγγιση αυτή έχει αυξήσει το χρόνο απόκρισης ενός IPS και, ενδεχομένως, δίνει στον εισβολέα αρκετό χρόνο για να πραγματοποιήσει τη ζημιά.

Το HIPS γίνεται όλο και περισσότερο μια αναγκαιότητα σε οποιοδήποτε περιβάλλον, στο σπίτι ή την επιχείρηση. Το HIPS έχει λύσεις για να κρατήσει το σύστημα σε μια γνωστή-καλή κατάσταση και αποτελεσματικά να αποφευχθεί το πρόβλημα των ψευδών συναγερμών.

Μια από τις πιο καινοτόμες εφαρμογές του HIPS είναι η SafenSoftSysWatch, όχι μόνο ειδοποιεί ζητήματα όταν άγνωστες εφαρμογές προσπαθούν να προωθηθούν, αλλά παρέχει κοκκώδη ελέγχους για το πώς διαφορετικές εφαρμογές μπορούν να έχουν πρόσβαση σε αρχεία και φακέλους, USB drives, τα κλειδιά μητρώου, εξωτερικές συσκευές, και των πόρων του δικτύου. Οι χρήστες μπορούν να δημιουργήσουν τους δικούς τους κανόνες HIPS για τον έλεγχο των δραστηριοτήτων εφαρμογών.

Network-based Intrusion Prevention Systems (HIPS)

Ένα δίκτυο με βάση το σύστημα ανίχνευσης πρόληψης (IPS) είναι ένα πρόγραμμα που εκτελεί σάρωση πακέτων και αναλύει την κυκλοφορία του δικτύου ώστε να εντοπίσει και να σταματήσει ύποπτη δραστηριότητα. Τα προϊόντα του NIPS τυπικά έχουν αναπτυχθεί σε σειρά, πράγμα που σημαίνει ότι οι [λογισμικό] πράξεις είναι σαν ένα τείχος προστασίας του δικτύου. Θα λαμβάνει τα πακέτα, τα αναλύει, αποφασίζει αν θα πρέπει να επιτρέπεται, και επιτρέπει να αποδέχεται την διέλευση πακέτων.

Η αρχιτεκτονική του NIPS επιτρέπει ορισμένες από τις επιθέσεις να ανιχνευθούν στα δίκτυα πριν φτάσει στους στόχους τους. Τα περισσότερα προϊόντα του NIPS χρησιμοποιούν ένα συνδυασμό των υπογραφών επίθεσης και της ανάλυση του δικτύου και την εφαρμογή πρωτοκόλλων, πράγμα που σημαίνει ότι θα συγκρίνουν τη δραστηριότητα του δικτύου για συχνές επιθέσεις εφαρμογών (π.χ., e-mail, διακομιστέςWeb) με την αναμενόμενη συμπεριφορά για να εντοπίζουν δυνητικά κακόβουλη δραστηριότητα.

Τα NIPS χρησιμοποιούνται για την ανίχνευση πολλών ειδών κακόβουλων δραστηριοτήτων εκτός από malware, και τυπικά μπορεί να ανιχνεύσει μόνο μερικά παραδείγματα των malware από προεπιλογή, όπως τα πρόσφατα μεγάλα worms. Ωστόσο, ορισμένα NIPS είναι υπερβολικά προσαρμοσμένα, επιτρέποντας στους διαχειριστές να δημιουργούν και να αναπτύσσουν υπογραφές επίθεση για πολλές μεγάλες νέες απειλές κακόβουλου λογισμικού μέσα σε λίγα λεπτά. Αν και υπάρχουν κίνδυνοι στο να γίνει αυτό, όπως μια κακώς γραπτή υπογραφή προκαλώντας ψευδώς αρνητικά που μπλοκάρουν καλοήθεις δραστηριότητα κατά λάθος, μια προσαρμοσμένη υπογραφή μπορεί να εμποδίσει μια νέα απειλή malware ώρες πριν οι υπογραφές antivirus γίνουν διαθέσιμες. Το NIPS μπορεί να σταματήσει αποτελεσματικά ειδικές γνωστές απειλές, όπως το δίκτυο υπηρεσιών worms , και e-mail που μεταδίδονται από worms και ιούς με εύκολα αναγνωρίσιμα χαρακτηριστικά (π.χ., θέμα, Όνομα σύνδεσης). Ωστόσο, το NIPS γενικά δεν είναι σε θέση να σταματήσει κακόβουλο κωδικό κινητού ή Trojanhorses. Το NIPS μπορεί να είναι σε θέση να ανιχνεύει και να σταματάει κάποιες γνωστές απειλές μέσω της ανάλυσης πρωτόκολλο εφαρμογής.

Τα NIPS, μπορούν να αναπτυχθούν σε διάφορα σημεία μέσα σε ένα δίκτυο για να υποστηρίξει τις οργανώσεις της συνολική στρατηγικής ασφάλειας του δικτύου. Αναπτυχθεί σε σειρά (blockingmode) στην περίμετρο του οργανισμού σας,

χρησιμοποιώντας υψηλού κινδύνου υπογραφές, μπορούν να παρέχουν ανταποκρίνεται μετριασμού για την εσωτερική περιουσιακών στοιχείων από τρωτών σημείων εφαρμογής γρηγορότερα από ό, τι ίσως οργανισμός σας μπορεί να αναπτύξει τα μπαλώματα. Ή ίσως, θέλετε να παρέχει επίπεδο εφαρμογής άμβλυνσης επίθεση DDOS για εταιρικές ιστοσελίδες που αντιμετωπίζει την αίτησή σας, και πάλι, η εγκατάσταση μιας συσκευής NIPS μπορεί να βοηθήσει.

Διαφορέςμεταξύ host-based και network-based IPS

Το σύστημα host-basedIPS μπορεί να λειτουργήσει με δύο κρυπτογραφημένα ή μη κρυπτογραφημένα δεδομένα, επειδή η ανάλυση γίνεται μετά όπου τα δεδομένα αποκρυπτογραφούνται από το σταθμό. Το σύστημα network-basedIPS δεν χρησιμοποιεί τη μνήμη και τον επεξεργαστή των σταθμών που τους προστατεύουν, αλλά έχει τη δική του μνήμη και επεξεργαστή. Το NIPS τοποθετείται στα κρίσιμα σημεία του δικτύου και το σύνολο της κυκλοφορίας εξαρτάται από την ορθή λειτουργία τους, η οποία μπορεί να είναι ένα μειονέκτημα, όταν ο εξοπλισμός δεν είναι λειτουργικός. Το NIPS μπορεί να ανιχνεύσει γεγονότα που διανέμονται στο δίκτυο (χαμηλή προτεραιότητα, αλλά τα γεγονότα που επηρεάζουν περισσότερους σταθμούς του δικτύου) και μπορεί να αντιδράσει, ενώ το HIPS έχει μόνο τα δεδομένα της συσκευής, όπου λειτουργούν, προκειμένου να είναι σε θέση να λάβουν μια απόφαση.

WirelessIntrusionPreventionSystems

Ένα ασύρματο IPS σαρώνει την ασύρματη κίνηση δεδομένων για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση ή επίθεση στο LAN και άλλους πόρους που χρησιμοποιούν την ασύρματη σύνδεση στο Internet. Ένα ασύρματο IPS παρακολουθεί το ραδιοφάσμα για την παρουσία ύποπτων σημείων πρόσβασης. Ανιχνεύει επίσης τη χρήση των ασύρματων μέσων επίθεσης. Μόλις ένα ασύρματο IPS ανιχνεύει ένα μη εξουσιοδοτημένο σημείο ασύρματης πρόσβασης, προειδοποιεί το δίκτυο ή το διαχειριστή του συστήματος ασφαλείας.

Ένα ασύρματο IPS έχει αναπτυχθεί με τη μορφή των αισθητήρων που περιέχουν κεραίες και τα ραδιόφωνα για τη σάρωση της ασύρματη κίνησης δεδομένων. Μετά ένας κεντρικός διακομιστής σαρώνει τα δεδομένα που συλλαμβάνονται από τους αισθητήρες.

3.1.3. Ψευδώς θετικά και αρνητικά των IPS

Στο πλαίσιο της πρόληψης ή εισβολής, ψευδώς θετικό είναι ένα IPS δηλώνοντας καλή κυκλοφορία ως κακή, με αποτέλεσμα είτε σε έναν ψευδή συναγερμό (αν οι IPS είναι σε παθητική λειτουργία ανίχνευσης) ή διακοπή υπηρεσίας (αν το IPS είναι σε υπό-έλεγχο λειτουργίας πρόληψης). Ένα ψευδώς θετικό συνήθως προκαλείται από ένα αναποτελεσματικό κανόνα IPS ή υπογραφή. Μια εσφαλμένη θετική δεν θα πρέπει να συγχέεται με μια «πραγματική» επίθεση που είναι αναποτελεσματική ενάντια στο λειτουργικό σύστημα ή εφαρμογή που στοχεύει. Για παράδειγμα, εάν έναConficker επιτίθεται σε ένα Linux υποδοχής, και ένα γεγονός εισβολής ενεργοποιείται, δεν είναι τεχνικά μια "ψευδής θετική», αλλά περισσότερο από ένα "δεν εφαρμόζεται", δεδομένου ότι Conficker επηρεάζει μόνο τα λειτουργικά συστήματα Windows.

Το αντίθετο πρόβλημα είναι με ένα ψευδώς αρνητικά, όταν ένα IPS αποτυγχάνει να αναγνωρίσει μια εισβολή ή άλλο γεγονός ασφαλείας. Αυτό μπορεί να συμβεί αν οι IPS δεν έχει ενημερώσει τους κανόνες, ή αν ο πωλητής IPS δεν έχει κυκλοφορήσει έναν κανόνα για ένα νέο είδος της επίθεσης ή της ευπάθειας. Όταν μια IPS τοποθετείται σε υπό-έλεγχο λειτουργικό κλειδώματος, ψευδώς αρνητικά αποτελέσματα είναι γενικά πολύ πιο επιζήμιες για έναν οργανισμό από ένα ψευδώς θετικό. Μια ψευδής αρνητική άδεια κακής κυκλοφορίας που μπορεί εισέλθει στο δίκτυο, μπορεί δυνητικά να οδηγήσει τα συστήματα σε κίνδυνο και ενδεχομένως να κλαπούν ή χαθούν τα δεδομένα. Ένα ψευδώς θετικό μπλοκάρισμα καλής κίνησης από την είσοδο του δικτύου, ενδέχεται να οδηγήσει σε απώλεια των επιχειρήσεων ή της παραγωγικότητας.[25]

3.1.4. Σύστημα πρόληψης εισβολών εναντίον firewalls

Το σύστημα IPS παρακολουθεί το σύστημα για τα ανεπιθύμητες εισόδους και αναφορές ή προειδοποιεί τον ίδιο το χρήστη και αποτρέπει τη σύνδεση. Ένα firewalls παρακολουθεί το σύστημα με βάση τους κανόνες που έχουν οριστεί από το χρήστη και ρυθμίζει τη δραστηριότητα μεταξύ του συστήματος και του διαδικτύου. Επίσης ένα firewalls μπορεί να περιορίσει την πρόσβαση σε ένα σύστημα υπολογιστή ή σε ένα δίκτυο υπολογιστών. Ελέγχει την κίνηση δεδομένων σε επίπεδο TCP / IP ports. Για παράδειγμα, ένα firewalls μπορεί να περιορίσει την πρόσβαση σε μια θύρα που δεν υπάρχει πρότυπο υπηρεσίας που χρησιμοποιεί.

Ωστόσο, αν ένας εισβολέας διαπερνά μέσα από μια τυπική θύρα όπως η θύρα 80 (που χρησιμοποιείται για HTTP) υπάρχει ένα μικρό firewalls που μπορεί να το αντιμετωπίσει. Firewalls συνήθως λειτουργούν μόνο για τα πακέτα που έρχονται στο δίκτυο ή μια σειρά. Επίσης, ένα IPS μπορεί να ανιχνεύσει την κίνηση σε πραγματικό χρόνο από τη σάρωση του μοτίβο της ροής δεδομένων από μια βάση δεδομένων τωνγνωστών μοντέλων επίθεση ή ένα τυποποιημένο πρότυπο δεδομένων. Ένα IPS μπορεί να ανιχνεύσει, επίσης, τόσο την εισερχόμενη και εξερχόμενη κίνηση ροή δεδομένων.

Αν συγκρίνετε ένα IPS και ένα firewalls σε ένα σύστημα ασφαλείας, θα μπορούσε να ειπωθεί ότι το firewalls ελέγχει μόνο τα δελτία ταυτότητας των πακέτων δεδομένων, αλλά το IPS ελέγχει τις αποσκευές. Επομένως, για την προστασία του συστήματος από ανεπιθύμητες εισβολές, συνιστάται πάντα να χρησιμοποιούν firewalls, σε συνδυασμό με το σύστημα αποτροπής εισβολών. Αυτό είναι και ο λόγος που η πλειονότητα των συστημάτων ασφαλείας συνοδεύονται από firewalls και IPS.[25]

3.1.5. Κορυφαία συστήματα IPS

Ossec	Είναι ένα δωρεάν σύστημα πρόληψης εισβολής. Εκτελεί ανάλυση καταγραφής, ελέγχου της ακεραιότητας, παρακολούθησης μητρώου των Windows, ανίχνευσης rootkit, χρόνο προειδοποίησης, και την ενεργό

	ανταπόκριση. Παρέχει ανίχνευσης πρόληψης για τα περισσότερα λειτουργικά συστήματα, όπως το Linux, OpenBSD, FreeBSD, Mac OS X, Solaris και Windows .
Suricata	Είναι ένα ανοιχτού κώδικα σύστημα πρόληψης εισβολής. Αναπτύχθηκεαπότην Open Information Security Foundation (OISF).

3.2. Εισαγωγή στο Ossec

Το OpenSourceSecurity (Ossec) είναι μια ανοικτή πηγή υποδοχής με βάση το σύστημα πρόληψης που εκτελεί αμφοτέρου το προφίλ και την υπογραφή με βάση την ανάλυση για την πρόληψη εισβολών στον υπολογιστή. Υποστηρίζεται από μια εταιρεία που ονομάζεται TrendMicro. Το σύστημα OSSEC αναπτύχθηκε αρχικά απότον DanielB. Cid για να αντισταθμίσει την έλλειψη της κλιμάκωσης της Tripwire (που χρησιμοποιούνται για τον έλεγχο της ακεραιότητας αρχείου).

Το σύστημα Ossec έχει διάφορα πλούσια χαρακτηριστικά και ισχυρή μηχανή ανάλυσης καταγραφής. Υποστηρίζει διάφορα πρωτόκολλα, servers και εφαρμογές. Έχει καταπληκτική ενεργό ανταπόκριση και ειδοποίηση για οποιαδήποτε παραβίαση της ασφάλειας. Το σύστημα Ossec παρέχει μια ποικιλία εργαλείων για τον υπολογιστή που βασίζεται σε πρόληψης εισβολής. Για παράδειγμα, το σύστημα Ossec μπορεί να εκτελέσει ανάλυση καταγραφής, έλεγχο της ακεραιότητας, την παρακολούθηση της πολιτικής.

Το σύστημα Ossec τρέχει στα περισσότερα λειτουργικά συστήματα, όπως το Linux, MacOS, Solaris, HP-UX, AIX και Windows.

3.2.1. Τι είναι το Ossec

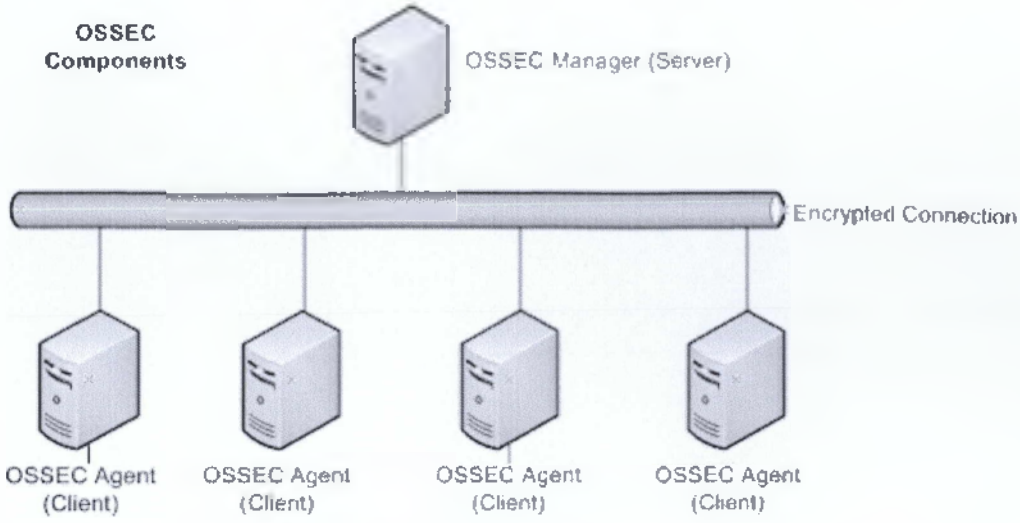
Το OpenSourceSecurity (Ossec) είναι ένα δωρεάν, ανοιχτού κώδικα σύστημα πρόληψης εισβολών. Το σύστημα Ossec έχει μια λίστα πελατών που περιλανβάνει εταιρείες υψηλού προφίλ, όπως το Netflix, Samsung, η Apple , Barnes&Noble , η NASA και άλλοι που χρησιμοποιούν OSSEC οι οποίες εκτελούν ανάλυση καταγραφής του συστήματος, κάνουν έλεγχο ακεραιότητας των αρχείων, παρακολούθηση της πολιτικής, ελέγχουν για αλλαγές στο μητρώο (για τα συστήματα Windows), ανίχνευση rootkit, το χρόνο προειδοποίησης, την ενεργό ανταπόκριση και αναλαμβάνουν δράσεις που βασίζονται σε συμβάντα ασφαλείας που εντοπίζονται.

Το σύστημα Ossec μπορεί να εγκατασταθεί ως αυτόνομο εργαλείο για την παρακολούθηση μιας υποδοχής ή μπορεί να αναπτυχθεί σε ένα σενάριο πολλαπλών ξενιστών, μία εγκατάσταση είναι ο διακομιστής και οι άλλες σαν παράγοντες. Ο διακομιστής και οι παράγοντες επικοινωνούν με ασφάλεια χρησιμοποιώντας κρυπτογράφηση. Το σύστημα Ossec είναι σε θέση να αντιδρά σε συγκεκριμένα γεγονότα ή εκδηλώσεις χρησιμοποιώντας εντολές και ενεργές αντιδράσεις. Τα συστήματα συνοδεύονται με κάποια προκαθορισμένα ενεργά μέσα αντιμετώπισης, αλλά οι διαχειριστές μπορούν και μόνοι τους.

Το σύστημα OSSEC λειτουργεί ως σύστημα πράκτορα-διακομιστή. Οι πράκτορες χειρίζονται την παρακολούθηση εισερχομένων, τα αρχεία και (Windows) μητρώα μετά στέλνει πίσω σχετικές καταγραφές σε κρυπτογραφημένη μορφή στο OSSEC διακομιστή μέσω UDP θύρα 1514 (θύρα). Στο διακομιστή τα αρχεία καταγραφής αναλύονται με αποκωδικοποιητές και ερμηνεύονται με κανόνες που δημιουργούν ειδοποιήσεις ασφαλείας που βρέθηκαν στο ρεύμα καταγραφής. Το σύστημα OSSEC συνοδεύεται με ένα πλούσιο σύνολο αποκωδικοποιητών και κανόνων για την παρακολούθηση σημαντικών γεγονότων του συστήματος, όπως οι αλλαγές στο αρχείο, συνδέσεις ως root, και πολλά άλλα. Οι χρήστες μπορούν να προσθέσουν προσαρμοσμένους αποκωδικοποιητές και κανόνες για την παρακολούθηση όλων των αρχείων και να δημιουργήσουν ειδοποιήσεις ειδικά για τις ανάγκες τους.[398]

OSSEC έχει δύο σημαντικά στοιχεία:

- OSSEC Manager (Server)
- OSSEC Agent (Client)



Εικόνα 6: Στοιχεία Ossec

Το σύστημα Ossec manager αποθηκεύει όλα τα δεδομένα που σχετίζονται με τον έλεγχο της ακεραιότητας, τις εισερχόμενες, τα γεγονότα, τους κανόνες, και επιλογές διαμόρφωσης για ολόκληρο το δίκτυο. Το σύστημα OSSECmanager συνδέεται με το OSSECagent και παίρνει όλες τις απαραίτητες πληροφορίες, ανεξάρτητα από το σύστημα λειτουργίας του. Και, φυσικά, όλες οι επικοινωνίες μεταξύ των διακομιστών και των πρακτόρων είναι κρυπτογραφημένη και ασφαλής.[40]

3.2.2. Δυνατότητες Ossec

Το σύστημα OSSEC έχει μια εξελιγμένη μηχανή ανάλυσης που εκτελεί τις ακόλουθες λειτουργίες:[41]

- Ανάλυση καταγραφής
- Έλεγχος ακεραιότητας
- Ανίχνευση ανωμαλιών
- Ανίχνευση rootkit
- Ενεργό ανταπόκριση

Ανάλυσηκαταγραφής

OSSEC περιλαμβάνει Log- based Intrusion Prevention System (LIPS). Αυτό έχει τη δυνατότητα να επανεξετάσει τα αρχεία καταγραφής σε σχεδόν πραγματικό χρόνο, ενώ περιεργάζονται γνωστά μοτίβα επίθεσης. Όταν ένα αρχείο καταγραφής δημιουργείται σε ένα προστατευμένο σύστημα, ο παράγοντας φροντίζει με ασφάλεια τη μετάδοση του log (κρυπτογράφηση Blowfish χρησιμοποιώντας ένα προ - κοινό μυστικό) στο διακομιστή. Ο διακομιστής στη συνέχεια λαμβάνει τη φροντίδα για την εκτέλεση της ανάλυσης.

Έλεγχος της ακεραιότητας

OSSEC περιλαμβάνει ένα εργαλείο που ονομάζεται Syscheck για την εκτέλεση αρχείων και καταλόγων ελέγχου της ακεραιότητας. Εάν εκτελείτε έναν παράγοντα των Windows, μπορείτε επίσης να περιλαμβάνετε συγκεκριμένα πλήκτρα στο μητρώο των Windows που πρέπει να παρακολουθούνται επίσης. Αλλαγές στο αρχείο μπορούν να ανιχνευθούν χρησιμοποιώντας τόσο MD-5 όσο και SHA-1 hash αλγορίθμων. Το σύστημα είναι εξαιρετικά προσαρμοσμένο. Μπορείτε να συμπεριλάβετε ή να εξαιρέσετε μόνο τα αρχεία ή ολόκληρες δομές καταλόγου. Μπορείτε να ορίσετε ακόμη και μια σημαία για τον εντοπισμό νέας δημιουργία αρχείου.

Ανίχνευση ανωμαλιών

OSSEC πηγαίνει πολύ πέρα από τις καταγραφές ελέγχου για να επιβεβαιώσει την ακεραιότητα του συστήματος. Πολιτικές χρήσης μπορεί να είναι η κεντρικήδιαχείριση από το διακομιστή, και στη συνέχεια να αναπτύσσεται προς τα έξω για τους κατάλληλους παράγοντες. Για παράδειγμα, μπορούμε να ορίσουμε μια πολιτική σχετικά με το ποιες εφαρμογές των Windows είναι αποδεκτές (Office, Firefox, κλπ) και ποιες δεν είναι (IM client, Skype, κ.λπ.). Μπορούμε να ορίσουμε ακόμη αποδεκτές επιλογές διαμόρφωσης, όπως επαληθεύοντας ότι τα NT hashes που χρησιμοποιούνται για τον κωδικό πρόσβασης αποθηκεύονται, αλλά όχι για τα LanManhashes.

Ανίχνευση rootkit

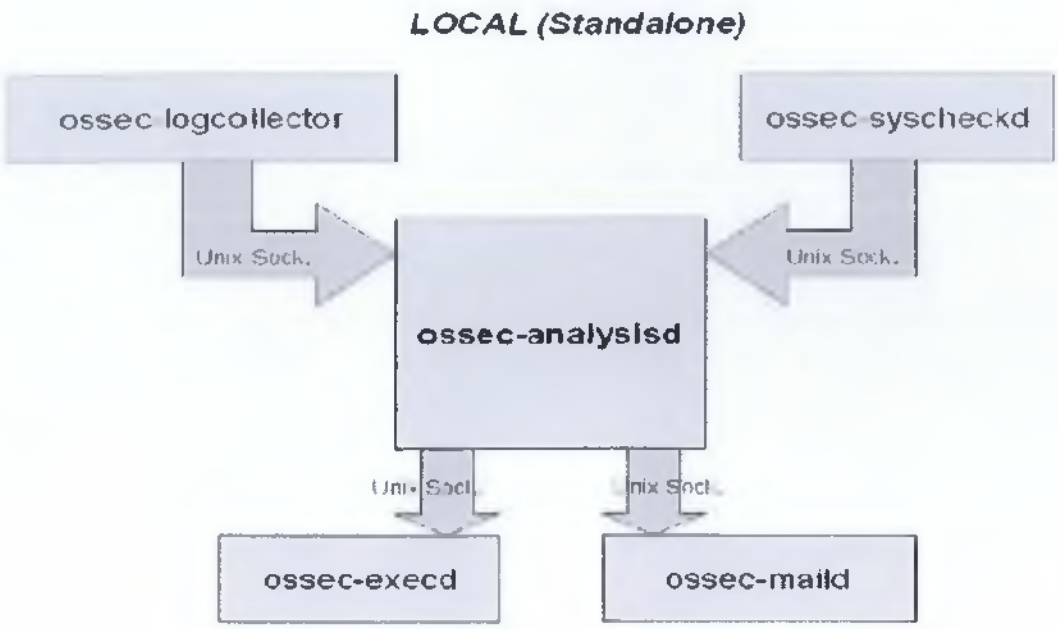
Χρησιμοποιούν πολλαπλές κλήσεις συστήματος για να προσπαθήσουν να ανοίξουν τα αρχεία για να επιβεβαιώσουν την ακεραιότητα και η λίστα υπογραφής περιέχεεί μέσα rootkit_files.txt αρχεία. Γίνεται έλεγχος για ανωμαλίες στους καταλόγους του συστήματος. Έλεγχος για κρυφές διαδικασίες. Έλεγχος για επιπόλαια διασύνδεση. Έλεγχος για κρυμμένες ανοικτές θύρες. Σαρώνει το σύστημα αρχείων και ψάχνει για αρχεία με περίεργα / επικίνδυνα δικαιώματα.

Ενεργό ανταπόκριση

OSSEC περιλαμβάνει την ικανότητα να ανταποκρίνεται κατά την ύποπτη δραστηριότητα που ανιχνεύεται. Οι απαντήσεις μπορούν να παραχθούν από τον διακομιστή ή τον παράγοντα, το οποίο ποτέ δεν το καθορίζουμε. Οι αντιγράσεις μπορεί να είναι καλοήθεις, όπως η δημιουργία ενός e-mail προειδοποίησης, για να είναι τόσο προληπτικός όσο το κλείδωμα μιας απομακρυσμένης διεύθυνσης IP για περιορισμένο χρονικό διάστημα.

3.2.3. Αρχιτεκτονική Ossec

Υπάρχουν δύο βασικοί τρόποι για να ρυθμίσετε OSSEC: Local και Server-Agent.



Εικόνα 7: Αρχιτεκτονική Ossec

Στην Local λειτουργία (που αναφέρεται επίσης ως Standalone λειτουργία), όλη η επεξεργασία OSSEC προκύπτει εντός του ενιαίου ξενιστή που παρακολουθούνται (βλέπε Σχήμα 7). Αυτό είναι χρήσιμο εάν υπάρχει μόνο ένας διακομιστής που πρέπει να παρακολουθείτε.

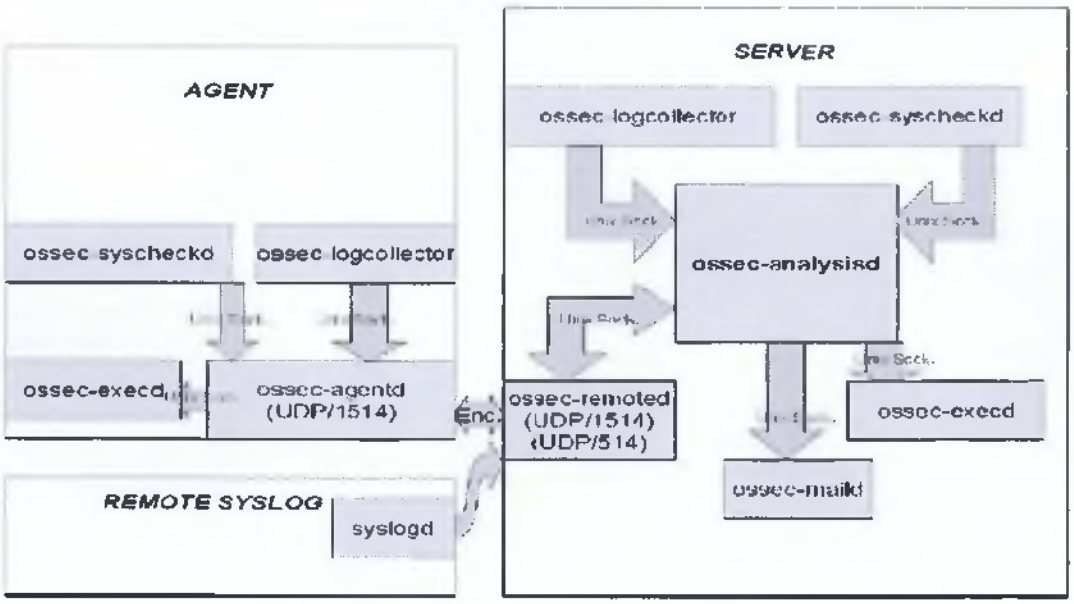
Οι διεργασίες που τρέχουν, ενώ η Local λειτουργεί είναι:

- ossec-logcollector (Διαβάζει τα αρχεία καταγραφής)
- ossec-syscheckd (Έλεγχος της ακεραιότητα του συστήματος και ανίχνευσης rootkit)
- ossec-analysisd (Μηχανή ανάλυσης)
- ossec-execd (Εκτελεί τις ενεργές δέσμες ενεργειών απόκρισης)
- ossec-maild (Αποστολή ειδοποιήσεων Email)

Χρησιμοποιεί το Ossec-Syscheckd για την παρακολούθηση του αρχείου για τις αλλαγές στο διακομιστή, καθώς και το τέλος παράγοντα. Η Ossec-Syscheckd παρακολουθεί επίσης (το ένα που είναι υπό παρακολούθηση) το αρχείο md5sum, ημερομηνία, άδειες αρχείων κλπ.

Η Ossec-Logcollector στο παράγοντα εισπράττει καταγραφές, περνάει τους Ossec-Agentd όπου με τη σειρά του περνάει τις καταγραφές καθώς και λεπτομέρειες όλων των γεγονότων μέσω των κρυπτογραφημένων κυκλοφοριών σε Ossec-Remoted που εκτελούνται στο διακομιστή. Όλες οι εκδηλώσεις στη συνέχεια πέρνάνε στους Ossec-Analysisd, το οποίο αποκωδικοποιεί και αναλύει τα αρχεία καταγραφής και όλες τις άλλες εκδηλώσεις. Όλες οι δραστικές αντιδράσεις χειρίζονται από το Ossec-Execd και ειδοποιήσεις μέσω email που αντιμετωπίζονται από Ossec-Maild, και τα δυο τρέχουν στο τέλος του διακομιστή.

Ωστόσο, οι περισσότεροι δικτυακοί τόποι επιλέγουν να παρακολουθήσουν μια σειρά από διακομιστές. Στην περίπτωση αυτή, προτείνεται η Server-Agent λειτουργία:



Εικόνα 8: Αρχιτεκτονική Ossec

Στη λειτουργία Server-Agent, ελαφρύ παράγοντες τρέχουν στους διακομιστές που παρακολουθούνται, και αυτά τα γεγονότα περνάνε μπροστά από το δίκτυο σε ένα ενιαίο, κεντρικό διακομιστή OSSEC (ο οποίος επίσης παρακολουθεί). Η μηχανή ανάλυσης τρέχει στον κεντρικό διακομιστή, ο οποίος δημιουργεί τις ειδοποιήσεις και στέλνει ειδοποιήσεις μέσω ηλεκτρονικού ταχυδρομείου.

Οι ίδιες διαδικασίες υπάρχουν στην λειτουργία Server-Agent όπως και στην Local λειτουργία, αλλά να περιλαμβάνει τα ακόλουθα, καθώς και:

- ossec-agentd [στον παράγοντα] Στέλνει Εκδηλώσεις στο διακομιστή

- ossec-remoted [στο διακομιστή] Λαμβάνει συμβάντα από τους παράγοντες
- ossec-monitord[στοδιακομιστή] Κατάσταση παρακολούθησης παραγόντων (δεν απεικονίζονται)

Αυτή η διαμόρφωση προτιμάται όταν παρακολουθεί πολλαπλούς διακομιστές διότι τα γεγονότα μπορεί να συσχετιστούν σε ξενιστές. Τι σημαίνει αυτό ότι το OSSEC έχει την ικανότητα να ανιχνεύει τύπων επιθέσεων που διαφορετικά περνάει απαρατήρητο από ένα HIDS αναλύοντας δεδομένα από ένα μόνο ξενιστή.

Ο Server-Agent ανάπτυξης είναι επίσης πιο εύκολο να διατηρηθεί. Οι ειδοποιήσεις κανόνων διαμένουν σε μόνο μία τοποθεσία, ειδοποιήσεις μέσω ηλεκτρονικού ταχυδρομείου προέρχονται από ένα μόνο μηχάνημα, κλπ.

Ένα πρόσθετο πλεονέκτημα είναι ότι η επεξεργασία ανάλυσης αποκαλύπτετε από τους διακομιστές παρακολούθησης. Ανάλογα με τον υφιστάμενο φόρτο εργασίας για την παρακολούθηση των μηχανημάτων, αυτό μπορεί να είναι ένας σημαντικός παράγοντας.

Το δίκτυο επικοινωνίας μεταξύ των παραγόντων και του διακομιστή είναι ασφαλής. Όλη η κυκλοφορία είναι κρυπτογραφημένη. Περαιτέρω, κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται για να διασφαλίσει την ακεραιότητα και προστασία της ιδιωτικής ζωής του OSSEC επικοινωνιών. Η διαδικασία για την προσθήκη κάθε νέου παράγοντα στο περιβάλλον του OSSEC περιλαμβάνει τη δημιουργία ενός δημόσιου / ιδιωτικού κλειδιού για τον διακομιστή, μετά την αντιγραφή και επικόλληση του δημόσιου κλειδιού στο παράγοντα.

Η OSSEC υποστηρίζει επίσης την κατάσταση στην οποία μόνο παρακολούθηση της καταγραφής είναι επιθυμητή (αλλά δεν ελέγχει την ακεραιότητα του συστήματος ή την ανίχνευση rootkit). Σε αυτή την περίπτωση, η εγκατάσταση syslog μπορεί απλά να σταλθεί στα αρχεία καταγραφής του σε όλο το δίκτυο (χωρίς κρυπτογράφηση) στον OSSEC διακομιστή και η OSSEC θα τους συμπεριλάβει στην ανάλυσή της. Αυτό παρουσιάζεται στο κάτω αριστερό παράθυρο του σχήματος 8.[42]

3.2.4. Υποστηριζόμενες πλατφόρμες

Το Ossec υποστηρίζεται από μεγάλο μέρος λειτουργικών συστημάτων. Την τρέχουσα στιγμή το Ossec είναι διαθέσιμα στα παρακάτω συστήματα:

- Linux
- MacOS
- Solaris
- HP-UX
- AIX
- Window

3.2.5. Κανόνες Ossec

Το σύστημα Ossec χρησιμοποιήσει τους διαμορφωμένους κανόνες για να καθορίσει εάν μια προειδοποίηση θα πρέπει να παραχθεί. Το Ossec έρχεται με ένα εκτεταμένο σύνολο κανόνων από προεπιλογή. Λόγω του ότι το Ossec μπορεί να εντοπίσει πάρα πολλά ενδεχόμενα συμβάντα έξω από το κουτί. Όμως, ο μεγάλος αριθμός των κανόνων επίσης μπορεί να προκαλέσει το Ossec να παράγει ένα εξίσου μεγάλο αριθμό λανθασμένων θετικών. Παρακάτω περιγράφονται τρεις κανόνες. Κάθε κανόνας που εμφανίζετε σχετίζεται με τον άλλο και η σχέση θα πρέπει να καθοριστεί.

```
<group name="syslog,sshd,">
 <rule id="5700" level="0" noalert="1">
  <decoded_as>sshd</decoded_as>
  <description>SSHD messages grouped.</description>
 </rule>

 <rule id="5710" level="5">
  <if_sid>5700</if_sid>
  <match>illegal user|invalid user</match>
  <description>Attempt to login using a non-existent
user</description>
  <group>invalid_login,authentication_failed,</group>
 </rule>

  <rule id="5712" level="10" frequency="6" timeframe="120"
ignore="60">
  <if_matched_sid>5710</if_matched_sid>
  <description>SSHD brute force trying to get access to
</description>
  <description>the system.</description>
  <same_source_ip />
  <group>authentication_failures,</group>
 </rule>
```

Εικόνα 9: Κανόνες Ossec

<grouptag>

Το <grouptag> δημιουργεί μια λογική ομαδοποίηση των κανόνων. Αυτό είναι για χρήση μέσα μόνο στο αρχείο ρυθμίσεων κανόνων.

<rule id>tag

Αυτή η ετικέτα συσχετίζεται με έναν αριθμό στον κανόνα. Η αριθμητική σειρά των κανόνων που περιλαμβάνονται είναι από 00000 έως 99.999. Προσαρμοσμένοι κανόνες θα πρέπει να κυμαίνεται από 100.000 έως 119.999. Εάν επιλέξατε ένα ID για έναν προσαρμοσμένο κανόνα, ο κανόνας μπορεί να είναι σε σύρραξη με τους κανόνες προεπιλογής.

Το rule ID tag είναι επίσης το επίπεδο του κανόνα που ορίζεται. Παρατηρείτε σημαντικά η κρισιμότητα των επιπέδων ενός κανόνα και η λειτουργία ως κατώτατο όριο για τις διάφορες εκθέσεις και λειτουργίες συναγερμού.Torule ID tag επίσης δεν μπορεί να συμπεριλαμβάνει την επιλογή της ειδοποίησης. Αυτό αποτρέπει ειδοποιήσεις από το να δημιουργούνται για το συγκεκριμένο κανόνα. Αυτό είναι ιδιαίτερα χρήσιμο για τον έλεγχο προσαρμοσμένων κανόνων ή προσωρινή αχρηστεύσει των κανόνων που χρειάζονται πρόσθετη ρύθμιση.

Η επιλογή συχνότητας χρησιμοποιείται για να μετρήσει τον αριθμό των εμφανίσεων μιας ιδιαίτερης αντιστοίχισης κανόνων. Πάντα φαίνεται με την επιλογή χρονοδιαγράμματος καθώς ο αριθμός των περιστατικών πρέπει να περιέχεται μέσα σε ένα καθορισμένο χρονικό πλαίσιο. Η επιλογή χρονοδιαγράμματος παρέχει ένα μηχανισμό για να περιοριστεί ο χρόνος στον οποίο ένας ορισμένος αριθμός καταγραφής μπορεί να καταχωρίσει ένα συγκεκριμένο κανόνα.

<decodedas>tag

Το decodedastag επιτρέπει το Ossec να γνωρίζει ποιον αποκωδικοποιητή να συνδέσει στον κανόνα.

<description>tag

Η descriptiontag παρέχει ένα χώρο για τον συγγραφέα των κανόνων να τονιστεί ο σκοπός του κανόνα. Το κείμενο που περιέχεται θα πρέπει σ 'αυτό να περιλαμβάνονται γεγονότα συναγερμού, εάν παράγονται.

<if_ sid>tag

Η if_sidtag δημιουργεί μια εξάρτηση σε ένα προηγούμενοο καθορισμένο κανόνα. Στο παραπάνω παράδειγμα, η if_sidtag κάνει κανόνα id 5710 που εξαρτάται από τον κανόνα 5700. Εάν ένας κανόνας 5700 δεν πυροδοτηθεί τότε ο κανόνας 5710 θα αγνοηθεί. Εάν ο κανόνας ID 5700 πυροδοτηθεί τότε ο κάθε κανόνας χαρακτηρίζεται ως εξαρτώμενος.

<match>tag

Η matchtag λειτουργεί ως ένα απλό παιχνίδι κειμένου. Εάν η σειρά καταγραφής περιέχει το κείμενο που σημειώνεται μέσα στην ετικέτα αγώνα, τότε ο κανόνας θα ενεργοποιηθεί. Σε αυτό το παράδειγμα, εάν το αρχείο καταγραφής περιέχει είτε «παράνομο χρήστη" ή "άκυρο χρήστη" (λόγω του χαρακτήρα καθέτου (|), ο κανόνας θα ενεργοποιηθεί.

<group>tag

Η grouptag χρησιμοποιείται για να καθορίσει μια υποομάδα εντός του κανόνα. Υπάρχουν και άλλα σημεία εντός του Ossec ότι κάποιος μπορεί να επιθυμεί να γίνει αναφορά σε μια συγκεκριμένη ομάδα κανόνων.

<if_ matched_ sid>tag

Αυτό συσχετίζει τον τρέχω κανόνα με τον προηγούμενο που ορίστηκε. Στην περίπτωση των κανόνων φαίνεται από τα παραπάνω, ο κανόνας 5712 συνδέεται με τον κανόνα 5710. Αυτό το φώλιασμα των κανόνων είναι απαραίτητο, ώστε να εξαρτώνται από τις συνθήκες που μπορεί να προκαλέσει ένα γεγονός.[43]

3.3. Εισαγωγή στο Suricata

Το σύστημα Suricata είναι μια ανοιχτή πηγή συστήματος πρόληψης εισβολών (IPS). Το σύστημα αναπτύχθηκε από την Open Information Security Foundation (OISF). OISF είναι ένας μη κερδοσκοπικό ίδρυμα , που χρηματοδοτείται από το DHS S&T και έχει προσελκύσει επίσης ιδιωτική χρηματοδότηση. Ο κινητήρας Suricata κυκλοφόρησε για πρώτη φορά το 2009 και το OISF συνεχίζει να συμμετάσχει ενεργά στον κυβερνοχώρο εμπειρογνωμόνων σε θέματα ασφάλειας και προγραμματιστές λογισμικού σε όλο τον κόσμο για να αναπτύξουν και να ενισχύσουν τα χαρακτηριστικά του κινητήρα.

Το Suricata είναι ένα επόμενης γενιάς υψηλής απόδοσης μηχανή ανοικτού κώδικα IPS με πολλά συν σε σχέση με άλλες λύσεις ανοικτού κώδικα. Μέσω της χρηματοδότησης της OISF, από το DHS S&T, έχει φέρει μια κοινότητα των ερευνητών του δικτύου και των φορέων και κορυφαίους προγραμματιστές λογισμικού ασφαλείας, και ενθάρρυνε τη συνεργασία και την καινοτομία, με βάση τις ανάγκες

της κοινότητας για την παραγωγή Suricata ώστε να λύσει τις προκλήσεις της ασφάλειας και να απαντήσει σε ανεκπλήρωτες ανάγκες στην IPS αγορά. Το σύστημα Suricata έχει πολλές βελτιώσεις και νέες λειτουργίες σε σχέση με άλλα παρόμοια λογισμικά.

Η Suricata μπορεί να αποκωδικοποιήσει TCP, UDP και ICMP, αλλά και HTTP, TLS, FTP και Samba. Ως μέθοδος εισαγωγής η Suricata μπορεί να πιάσει τα πακέτα με μια τυπική ακατέργαστη υποδοχή ή NFQueue, PCAP και IPFring. Οι τελευταίες μεθοδολογίες που έχει δημιουργήσει από PF_RING είναι ένα είδος υποδοχής δικτύου ειδικά κατασκευασμένο για να βελτιώνει την ταχύτητα λήψης πακέτων. Η Suricata τρέχει στα λογισμικά Mac OS X, Linux, BSD και Windows.[44]

3.3.1. Τι είναι το Suricata

Suricata είναι ένα σύστημα πρόληψης εισβολών (IPS), και δίκτυο παρακολούθησης της ασφάλειας του κινητήρα που αναπτύχθηκε από το OpenInformationSecurityFoundation (OISF). Το σύστημα Suricata ενσωματώνει χαρακτηριστικά που πηγαίνουν πέρα από την παραδοσιακή υπογραφή που βασίζονται στην πρόληψη και βελτιώνει σημαντικά τις επιδόσεις .

Το Suricata είναι ένας κανόνας που βασίζεται στον κινητήρα που χρησιμοποιείται εξωτερικά ώστε να αναπτυχθούν κανόνες που ορίζουν την παρακολούθηση της κίνησης του δικτύου και για να παρέχουν ειδοποιήσεις στο διαχειριστή του συστήματος, όταν συμβαίνουν ύποπτα συμβάντα. Για να είναι συμβατός ο σχεδιασμός με τα υπάρχοντα στοιχεία ασφάλειας του δικτύου, το Suricata διαθέτει ενιαία λειτουργικότητα παραγωγής και αποσπώμενες επιλογές στην βιβλιοθήκη για να δέχεται κλήσεις από άλλες εφαρμογές. Όταν εισαχθεί ένα πακέτο στο σύστημα τότε το σύστημα Suricata συλλαμβάνει το πακέτο, το αποκωδικοποιεί, το επεξεργάζεται και τέλος το αναλύει.

Το Suricata είναι μοναδικό, δεδομένου ότι μπορεί να υποστηρίξει υψηλής απόδοσης πολλαπλών-πυρήνων και πολλαπλών-επεξεργαστών συστήματα. Τα κυριότερα οφέλη ενός multi-threaded σχεδιασμό είναι ότι προσφέρει αυξημένη ταχύτητα και αποτελεσματικότητα στην ανάλυση της κίνησης του δικτύου. Εκτός από την

επιτάχυνση υλικού (με περιορισμούς υλικού και κάρτα δικτύου), ο κινητήρας έχει κατασκευαστεί για να αξιοποιήσει την αυξημένη επεξεργαστική ισχύ που προσφέρονται από τους τελευταίους πολλαπλούς-πυρήνες συνόλων CPU.

3.3.2. Δυνατότητες Suricata

Υπάρχουν τρεις λόγοι για τους οποίους μπορούμε να χρησιμοποιήσουμε το σύστημα Suricata:[45]

- Εξαιρετικά επιδεκτικός διεύρυνσης
- Ταυτοποίηση πρωτοκόλλου
- Αναγνώριση αρχείου, MD5 Checksums, και εξαγωγή αρχείων

Εξαιρετικά επιδεκτικός διεύρυνσης

Suricata είναι multi-threaded. Αυτό σημαίνει ότι μπορεί να εκτελεστεί μία περίπτωση και θα εξισορροπήσει το φορτίο της επεξεργασίας σε κάθε επεξεργαστή σε έναν αισθητήρα Suricata που έχει ρυθμιστεί για χρήση. Αυτό επιτρέπει σε αγαθό εξοπλισμού την επίτευξη 10 Gigabit ταχύτητες για την πραγματική κυκλοφορία της ζωής χωρίς να θυσιάζει την κάλυψη.

Ταυτοποίηση πρωτοκόλλου

Τα πιο κοινά πρωτόκολλα αναγνωρίζεται αυτόματα από το Suricata καθώς το ρέμα ξεκινά, επιτρέποντας έτσι στους συγγραφείς κανόνων να γράφουν έναν κανόνα του πρωτοκόλλου, όχι για την αναμενόμενη θύρα. Το γεγονός αυτό καθιστά το Suricata μια εντολή malware και κανάλι ελέγχου που δεν μοιάζει με καμία άλλη. Από τη θύρα HTTP κανάλια CnC, η οποία κανονικά ολισθένει δεξιά από τα περισσότερα συστήματα.

Αναγνώριση αρχείου, MD5 Checksums, και διεξαγωγή αρχείων

Suricata μπορεί να εντοπίσει χιλιάδες είδη αρχείων κατά τη διέλευση του δικτύου. Όχι μόνο μπορεί να το εντοπίσει, αλλά θα πρέπει να αποφασίσει ότι θέλει να το εξετάσει περαιτέρω, μπορεί να το επισημάνει για την εξαγωγή και το αρχείο θα γραφτεί στο δίσκο με ένα δεδομένο αρχείου που περιγράφει την κατάσταση της

σύλληψης και της ροής. MD5 checksum του αρχείου υπολογίζεται onthefly, έτσι εάν έχετε μια λίστα με MD5 hashes που θέλετε να κρατήσετε στο δίκτυό σας, ή θέλετε να κρατήσετε έξω, το σύστημα Suricata μπορεί να το βρει.

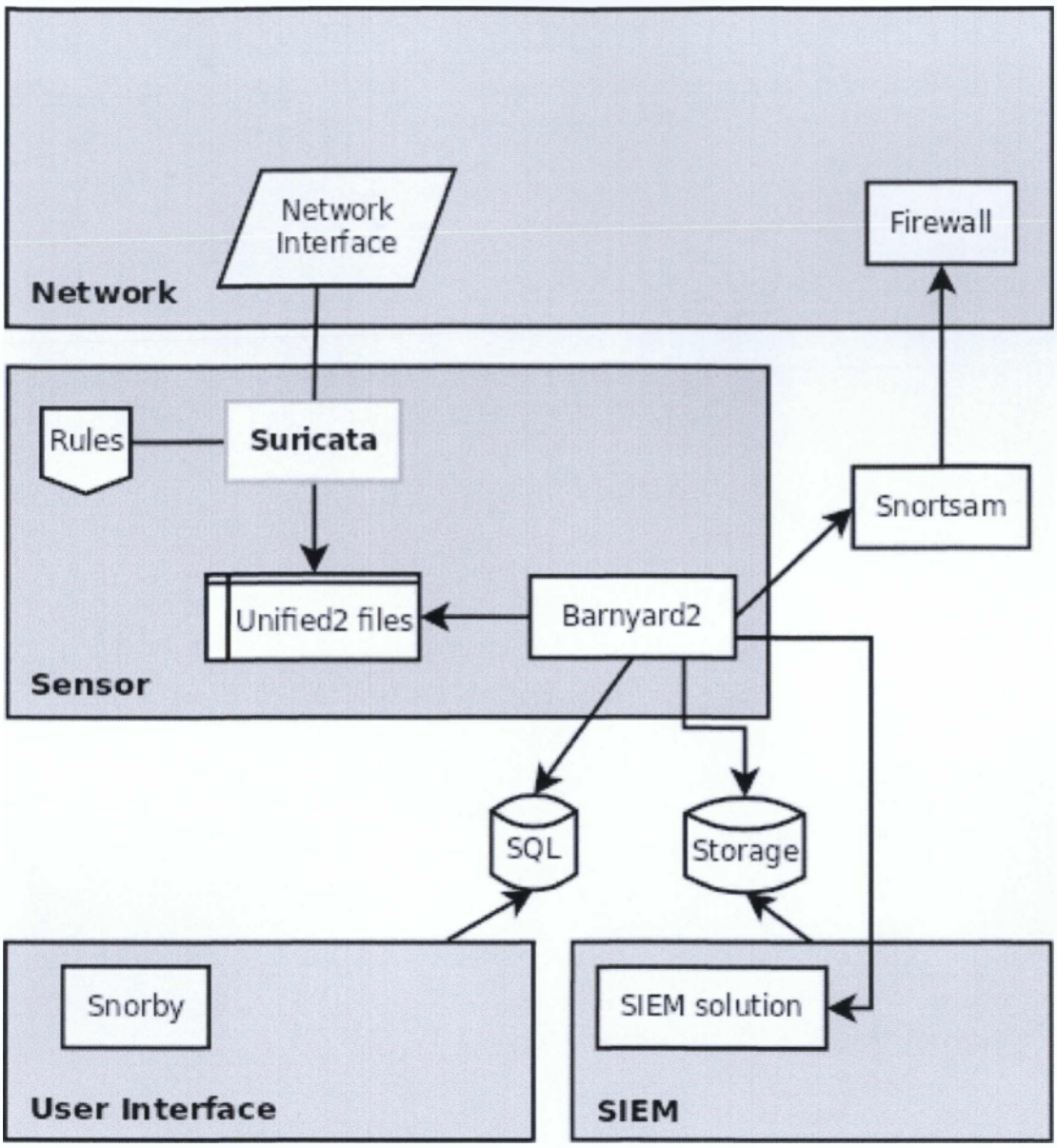
3.3.3. Πλεονεκτήματα Suricata

Το σύστημα Suricata, μια μηχανή IPS, προσφέρει πολλά οφέλη για την καταπολέμηση απειλών για την ασφάλεια του σήμερα. Το σύστημα Suricata είναι μια ανοιχτή πηγή μηχανής. Αυτή η δύναμη της κοινότητας λειτουργεί καλά μέσα σε IT άμυνες ασφαλείας, ως κοινότητα είναι πιο αποτελεσματική από μια ενιαία οργάνωση σε σύλληψη χαρακτηριστικά των αναδυόμενων απειλών. Επίσης, μια αρχιτεκτονική multi-threaded επιτρέπει να εκμεταλλευτεί τους πολλαπλούς πυρήνες και τις πολλαπλές αρχιτεκτονικές συστημάτων.

Το Suricata μπορεί και υποστηρίζει IP φήμη, όπου με την ενσωματώσει της φήμης και τις υπογραφές στη μηχανή, το Suricata μπορεί να επισημάνει την κυκλοφορία από τις γνωστές κακές πηγές. Ακόμα, μπορεί να ανιχνεύει αυτοματοποιημένα πρωόκολλα δηλαδή οι προεπεξεργαστές εντόπιζαν αυτόματα το πρωτόκολλο που χρησιμοποιείται σε ένα ρέμα του δικτύου και την εφαρμογή των κατάλληλων κανόνων, ανεξάρτητα από την αριθμητική θύρα. Η αυτόματη ανίχνευση πρωτοκόλλου αποτρέπει επίσης τα λάθη των χρηστών και τα λάθη που στην πραγματικότητα είναι πιο συχνές.

3.3.4. Σύστημα Suricata

Suricata είναι ένα IPS κινητήρα. Για να οικοδομήσουμε μια ολοκληρωμένη λύση, θα πρέπει να χρησιμοποιήσουμε άλλα εργαλεία. Το ακόλουθο σχήμα είναι μια αναπαράσταση μιας πιθανής εγκατάστασης του λογισμικού στην περίπτωση Suricata χρησιμοποιείται ως IPS στο δίκτυο. Χρησιμοποιεί μόνο ανοιχτές πηγές στοιχεία:



Εικόνα 10: Σύστημα Suricata

Suricata χρησιμοποιείται για την όσφρηση και την ανάλυση της κυκλοφορίας. Για την πρόληψη κακόβουλης κίνησης, που χρησιμοποιεί υπογραφές (ή κανόνες).

Για να αναλύσει τις ειδοποιήσεις που δημιουργούνται από Suricata, θα χρειαστείτε ένα περιβάλλον, όπως, για παράδειγμα, snorby. Αλλά αυτή η διασύνδεση θα πρέπει να έχει πρόσβαση στα δεδομένα. Αυτό γίνεται με την αποθήκευση των καταχωρήσεων σε μια βάση δεδομένων. Η τροφοδοσία της βάσης δεδομένων μπορεί να γίνει με barnyard2 που λαμβάνει τα αρχεία που εξάγονται από Suricata το unified2 και τη μετατροπή και να τα στείλει σε μια βάση δεδομένων (ή σε κάποια άλλη μορφή).[46]

3.3.5. Υποστηριζόμενες πλατφόρμες

Το Suricata υποστηρίζεται από μεγάλο μέρος λειτουργικών συστημάτων. Την τρέχουσα στιγμή το Suricta είναι διαθέσιμα στα παρακάτω συστήματα:

- Mac OS X
- Linux
- Freebsd
- Windows
- UNIX

Κεφάλαιο 4: Υβριδικά συστήματα ανίχνευσης και πρόληψης

4.1. Υβριδικό σύστημα

Έχει διαπιστωθεί ότι η ικανότητα ελέγχου (monitoring) των τρεχόντων συστημάτων ανίχνευσης εισβολών μπορεί να βελτιωθεί με την υιοθέτηση μια υβριδικής μεθόδου που αποτελείται ταυτόχρονα και από τις στρατηγικές ανίχνευσης διαταραχών καθώς επίσης και των υπογραφών. Ένα υβριδικό ή σύνθετο (hybrid ή compound) σύστημα ανίχνευσης συνδυάζει και τις δυο παραπάνω προσεγγίσεις. Ένα υβριδικό σύστημα ανίχνευσης είναι ένα κατά την υπογραφή εμπνευσμένο (signatureinspired) σύστημα ανίχνευσης εισβολών που λαμβάνει μια απόφαση χρησιμοποιώντας ένα '' υβριδικό πρότυπο'' που είναι βασισμένο και στην κανονική συμπεριφορά (normalbehavior) του συστήματος και στην παρεισφρητική συμπεριφορά (intrusivebehavior) των εισβολέων.

Σε ένα υβριδικό σύστημα, η τεχνική ανίχνευσης διαταραχών ενισχύει την ανίχνευση νέων ή άγνωστων επιθέσεων ενώ η τεχνική ανίχνευσης κακής συμπεριφοράς ανιχνεύει τις γνωστές επιθέσεις. Ακόμα, η τεχνική ανίχνευση υπογραφών είναι σε θέση να ανιχνεύσει τις επιθέσεις που προωθούνται από έναν επίμονο επιτιθέμενο που προσπαθεί να αλλάξει την συμπεριφορά των σχεδίων-προτύπων (patterns) με στόχο την επανεκπαίδευση της ενότητας (module) της ανίχνευσης διαταραχών έτσι ώστε θα δεχτεί τη συμπεριφορά της επίθεσης ως κανονική.

Αν και ο συνδυασμός των πολλαπλών τεχνολογιών ανίχνευσης εισβολών σε ένα ενιαίο σύστημα μπορεί θεωρητικά να παράγει ένα πολύ ισχυρότερο σύστημα ανίχνευσης εισβολών, τα προκύπτοντα υβριδικά συστήματα δεν είναι πάντα καλύτερα. Οι διαφορετικές τεχνολογίες ανίχνευση εισβολών εξετάζουν την κυκλοφορία των συστημάτων ή και των δικτύων και ψάχνουν την παρεισφρητική δραστηριότητα (intrusiveactivity) με διαφορετικούς τρόπους. Άρα, η σημαντικότερη πρόκληση στην οικοδόμηση ενός λειτουργικού υβριδικού συστήματος ανίχνευσης εισβολών είναι το να πάρει και να αξιοποιήσει αυτές τις διαφορετικές τεχνολογίες για αποτελεσματικότερη και αποδοτικότερη επικοινωνία διαλειτουργικότητα (interoperation).Σε γενικές γραμμές, τα συστήματα ανίχνευσης που βασίζονται αποκλειστικά σε υπογραφές δεν μπορούν να ενεργοποιήσουν μια άμυνα ενάντια προηγουμένων άγνωστων επιθέσεων. Από την άλλη πλευρά, η ανωμαλία που βασίζονται σε κομψότητα μπορεί να αναγνωρίσει τη νέα συμπεριφορά, αλλά συχνά

είναι ανίκανο να διακρίνει μεταξύ των προηγουμένων απαρατήρητων καλών συμπεριφορών και προηγουμένων απαρατήρητων κακών συμπεριφορών.[15]

Μια υβριδική προσέγγιση στην ανίχνευση μπορεί να παρέχει τη βάση για ένα σύστημα πρόληψης εισβολών (IPS): ένα αυτοματοποιημένο αντιδραστικό σύστημα ικανό για να σταματήσει μια επίθεση από την επιτυχία. Ο πυρήνας του υβριδικού συστήματος μας είναι μια ανωμαλία που βασίζεται σε κομψότητα που ενσωματώνει εποικοδομητική κριτική και στα δυο συντονιστικό πρότυπο και να δημιουργεί αυτόματα υπογραφές γνωστών κακόβουλων συμπεριφορών.

Στο παρελθόν, οι τεχνικές εξόρυξης δεδομένων, όπως η χρήση κανόνων συσχέτισης προτάθηκαν για την κατασκευή IDS Lazarevicetal για να διακρίνουν τις διαφορές μεταξύ των μοναδικών-συνδέσεων και πολλαπλών επιθέσεων σύνδεσης. Και οι δύο βάση υπογραφής και βάση ανωμαλιών IDSs είναι ευαίσθητοι στα χαρακτηριστικά της επίθεσης, το ιστορικό σύστημα εκπαίδευσης, τις παρεχόμενες υπηρεσίες, και υποκείμενες συνθήκες δικτύου. Οι τεχνικές εξόρυξης δεδομένων επίσης χρησιμοποιούνται για την κατασκευή μοντέλων ταξινόμησης από την ετικέτα επιθέσεις. Ανίχνευση εισβολών θα πρέπει να σχεδιαστεί για να παρακολουθεί τα χαρακτηριστικά της σύνδεσης στο δίκτυο, τις μεταφορές, και τα στρώματα εφαρμογής. [17]

Η ιδέα των συχνών κανόνων κεφαλαίου (FERs) προτάθηκε για πρώτη φορά από τους Mannila και Toivonen. Στη συνέχεια, ο Leeetal πρότεινε ένα πλαίσιο για να καθορίσει μεταβιβάσεις για την ανίχνευση ανωμαλιών εναντίων συνηθισμένων προφίλ της κυκλοφορίας. Ανέπτυξαν ένα επίπεδο σοφού αλγορίθμου εξόρυξης δεδομένων για τη δημιουργία ADS. Ο Fanetal παρατεταμένος από τον Leeetal 's εργάστηκε για να ανακαλύψει το ακριβές όριο μεταξύ γνωστών επιθέσεων και άγνωστων ανωμαλιών. Qin και Hwang προτείνανε έναν προσαρμοστικό βάση στήριξης αλγόριθμο για την εξόρυξη του κανονικού συνόλου δεδομένων. Kaleton Internet έχτισε ένα πρωτότυπο σύστημα με το συνδυασμό των δύο συστημάτων ανίχνευσης, αλλά λειτουργούν ανεξάρτητα χωρίς αλληλεπιδράσεις.

Θεωρούμε στενή συνεργασία μεταξύ των δύο υποσυστημάτων. Στην εργασία αυτή, προτείνουμε την υβριδική αρχιτεκτονική συστήματος ανίχνευσης εισβολών.

Για την βάση υπογραφών το σύστημα καθορίζει τα χαρακτηριστικά από τις παρατηρήσεις, καθώς από τις παρατηρήσεις και τις προηγούμενες ετικέτες και εκτελεί ακολουθία επισήμανσης μέσω των CRFs των ετικετών κάθε χαρακτηριστικού στην παρατήρηση. Αυτή η ρύθμιση είναι επαρκής για τη διαμόρφωση της συσχέτισης μεταξύ των διαφορετικών χαρακτηριστικών μιας παρατήρησης.

Αυτό το σύστημα, ενσωματώνει επίσης το EncrustedApproach με τις CRFs για να αποκτήσει τα οφέλη της υπολογιστικής απόδοσης και υψηλή ακρίβεια ανίχνευσης σε ένα ενιαίο σύστημα. Για την βάση ανωμαλιών το σύστημα θα ερευνήσει τα σχέδια του χρήστη, όπως το προφίλ των προγραμμάτων που εκτελούνται καθημερινά ή τις προνομιούχες διαδικασίες εκτελούνται με την πρόσβαση στους πόρους που είναι απρόσιτες για τους απλούς χρήστες με τη συλλογή των πτητικών στοιχείων από το σύστημα. Στη συνέχεια, εκπαιδεύουμε το σύστημά χρησιμοποιώντας όρους τυχαίων πεδίων, η οποία μειώνει το ποσοστό των λανθασμένων συναγερμών.

Ένα σύστημα αναγνώρισης επιθέσεων βασισμένο σε αυτήν την αρχιτεκτονική κάνει χρήση δυο ή και περισσότερων από αυτές τις αρχιτεκτονικές, έτσι ώστε να εκμεταλλευτεί τα πλεονεκτήματα της μιας για να καλύψει τις αδυναμίες της άλλης. Για παράδειγμα, ο Sekar συνδύασε στατιστικές μεθόδους για αναγνώριση ανωμαλιών με μια μηχανή καταστάσεων που καθορίζουν την επιτρεπόμενη δικτυακή επικοινωνία.

Το μεγαλύτερο εμπόδιο για ένα υβριδικό σύστημα είναι η πηγή εποικοδομητικής κριτικής πληροφόρησης. Στην ιδανική περίπτωση, θα πρέπει να είναι αυτοματοποιημένες και ολοφάνερες για τους χρήστες.

4.1.1. Υβριδική λειτουργία

Ένας συνδυασμός δύο ή περισσότερων BouncerDefenseUni (BDUs), αναπτύσσεται σε διαφορετικούς τρόπους, που εργάζονται από κοινού, προκειμένου να συλλέξει στοιχεία και να αποτραπεί εισβολές. Μπορείτε να αναπτύξετε αυτές τις BDUs σε διαφορετικά τμήματα του δικτύου προστατευόμενων ενώ χρησιμοποιείτε μια ενιαία κονσόλα διαχείρισης (BCU).

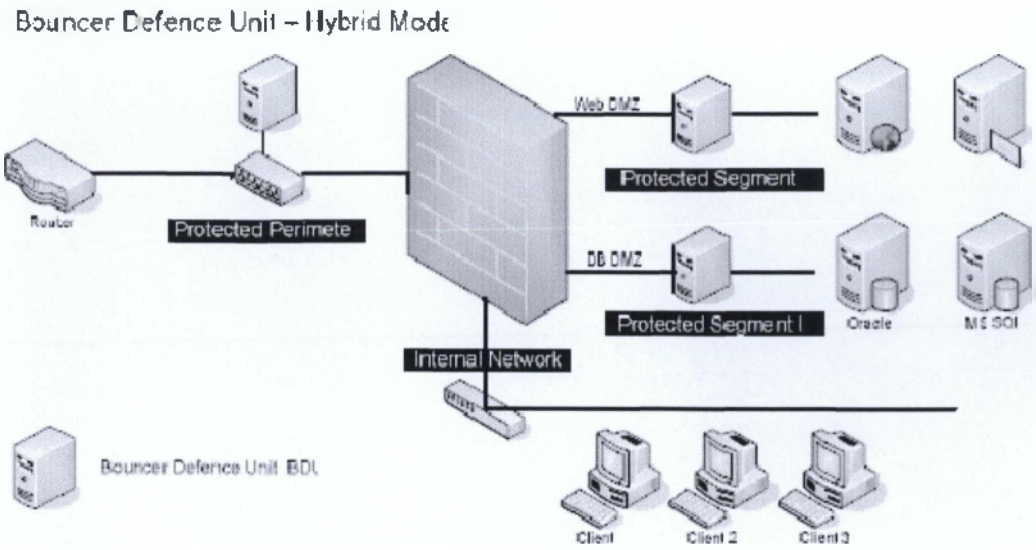
Υβριδική λειτουργία φαίνεται στο Σχήμα 11. Η λειτουργία αυτή συνδυάζει την διάρκεια και inline διαμόρφωση. Η BDU περίμετρος αναπτύχθηκε για να παρακολουθεί όλα τα κατεβάσματα του δικτύου, κυρίως για τη συλλογή αποδεικτικών στοιχείων, ενώ οι BDUs προστατεύει τα τμήματα που εμφανίζονται για να εμποδίσουν τις επιθέσεις. Το inlineBDUs μπορεί να ρυθμιστεί ώστε να παράγει πλαστά ή αργή ανταπόκριση, για να μπερδεύουν τον εισβολέα και να επιβραδύνει την επίθεση. Στην περίπτωση αυτή, η BDU στην περίμετρο μπορεί να παρέχει πρόσθετο χρόνο για να συγκεντρώσει περισσότερες πληροφορίες στον επιτιθέμενο και στην ίδια τη επίθεση.[2]

Παραδείγματα χρήσης:

- Λειτουργία έρευνας: συγκέντρωση αποδεικτικών στοιχείων και ύποπτη δραστηριότητα από το ένα τμήμα, ενώ την πρόληψη επιθέσεων από την άλλη.
- Ενεργό honey-pot.
- Δίκτυο παρακολούθησης της κυκλοφορίας και της πρόληψης.

Πλεονεκτήματα:

- Ενιαία αντικατάσταση των τρέχων IDS.
- Δεν δημιουργεί επιπλέον σημείο αποτυχίας.
- Απαιτούνται ελάχιστες αλλαγές στο δίκτυο.
- Αξιοποιεί πλήρως την προώθηση πολιτικής Bouncerlogic-to-log, και ανακόπτει την κυκλοφορία.
- Συνδυάζει την πρόληψη με τη συλλογή στοιχείων.



Εικόνα 11: Υβριδική λειτουργία

4.1.2. Πλεονεκτήματα και μειονεκτήματα Hybrid

Τα υβριδικά συστήματα έχουν πλεονεκτήματα και μειονεκτήματα. Τα πλεονεκτήματα τους είναι ότι έχουν ανώτερη προστασία για τα γνωστά και για τα zerodays απειλές. Ακόμα, κάθε υβριδικό παίζει από την αδυναμία του άλλου. Τα μειονεκτήματα τους είναι ότι είναι πιο ακριβά από οποιαδήποτε βάση ανωμαλιών ή βάση υπογραφών προϊόντων. Επιπλέον, μπορεί να εξαρτάται από την αρχιτεκτονική πιο αργά.[47]

4.1.3. Υβριδική αρχιτεκτονική συστήματος

Για τη βελτίωση της παραγωγικότητας της κατάχρησης και την ανίχνευση ανωμαλιών, αρκετά υβριδικά συστήματα ανίχνευσης εισβολών έχουν προταθεί. Τα πλαίσια αυτά συνδυάζουν την κατάχρηση και την ανίχνευση ανωμαλιών για να επιτευχθεί το ποσοστό ανίχνευσης της κατάχρησης ανίχνευσης και για την ανίχνευση άγνωστων εισβολών. Υπάρχουν τρεις τρόποι για να συνδυάσει κατάχρηση και ανίχνευση ανωμαλιών: αρχικά χρήση ανίχνευσης ανωμαλίας μετά την ανίχνευση κακής χρήσης, χρήση κατάχρηση και ανίχνευση ανωμαλιών παράλληλα και χρήση κατάχρησης ανίχνευσης και έπειτα ανίχνευση ανωμαλιών.

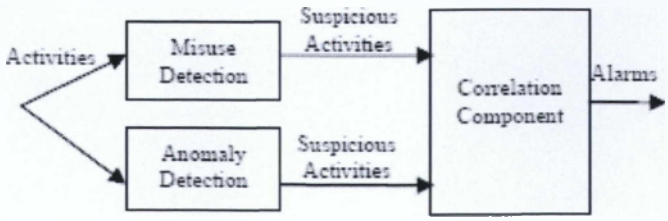
Κάποια υβριδικά συστήματα ανίχνευσης εισβολής χρησιμοποιούν ανίχνευση ανωμαλίας αρχικά για τον εντοπισμό καχύποπτων δραστηριοτήτων και μετά χρησιμοποιούν τη λειτουργία ανίχνευσης κακής χρήσης για την ανίχνευση επιθέσεων

από καχύποπτες δραστηριότητες. Ύποπτες δραστηριότητες είναι εκείνες που αποκλίνουν από το προφίλ της συνηθισμένης δραστηριότητας. Το πλαίσιο αυτής της προσέγγισης απεικονίζεται στο Σχ. 12. Παρατηρήθηκαν δραστηριότητες που εφαρμόζονται στην ανίχνευση ανωμαλίας για να παράγουν τις ύποπτες δραστηριότητες και μετά ανίχνευση κακής χρήσης χρησιμοποιείται για την ανίχνευση επιθέσεων. Οι συνδέσεις οι οποίες ταιριάζουν με το σχέδιο της επίθεσης έχουν ετικέτα ως επίθεση, εκείνα που ταιριάζουν σε ψευδείς σχέδια συναγερμού έχουν ετικέτα ως φυσιολογική και οι υπόλοιπες χαρακτηρίζονται ως άγνωστες επιθέσεις.

Εικόνα 12: Διαπίστωσης ανωμαλίας κατά την πρώτη κατάχρηση μετά την ανίχνευση

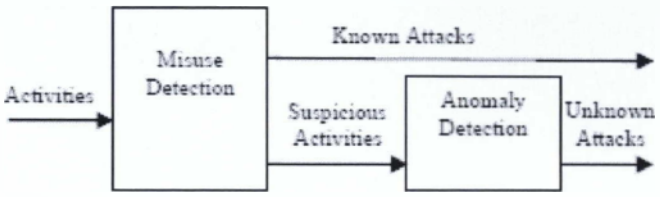
Σε υβριδικά συστήματα ανίχνευσης εισβολής που χρησιμοποιούν την ανίχνευση ανωμαλιών σε πρώτη φάση, για τη μείωση των ψευδών θετικών ποσοστών πλαισίου, το στοιχείο αυτό πρέπει να έχει υψηλό ποσοστό ανίχνευσης και η ανίχνευση κατάχρησης στοιχείου πρέπει να έχει την ικανότητα να ανιχνεύει το ποσοστό ψευδών θετικών. Έτσι, αυτά τα πλαίσια δεν θα είναι κατάλληλα για τα υβριδικά συστήματα ανίχνευσης εισβολής. Στο Σχήμα 12 δείχνει το πλαίσιο αυτών των υβριδικών συστημάτων.

Κάποια υβριδικά συστήματα ανίχνευσης εισβολής χρησιμοποιούν ανίχνευση κατάχρησης και ανίχνευση ανωμαλίας στοιχείου παράλληλα. Σε αυτά τα πλαίσια και τα δύο στοιχεία δημιουργούν ύποπτες δραστηριότητες ξεχωριστά. Μετά, το στοιχείο συσχέτισης χρησιμοποιείται για να αποσπάσει εισβολές από ύποπτες δραστηριότητες. Στο Σχήμα 13 δείχνει το πλαίσιο αυτών των υβριδικών συστημάτων.



Εικόνα 13: Παράλληλη προσέγγιση

Άλλα υβριδικά συστήματα ανίχνευσης εισβολής απασχολούν ανίχνευση κατάχρησης αρχικά και τη χρήση ανίχνευση ανωμαλιών έπειτα. Αυτά τα πλαίσια μπορούν να ανιχνεύσουν γνωστές επιθέσεις σε πραγματικό χρόνο και να δημιουργήσουν ύποπτες δραστηριότητες από τις ακόλουθες δραστηριότητες. Ανίχνευση ανωμαλίας χρησιμοποιείται για την ανίχνευση άγνωστων εισβολών από τις ύποπτες δραστηριότητες.[3]



Εικόνα 14: Ανίχνευση κατάχρηση αρχικά μετά ανίχνευση ανωμαλιών

4.1.4. Προτεινόμενη υβριδική αρχιτεκτονική

Η κατάχρηση ανίχνευσης έχει υψηλό ποσοστό ανίχνευσης για γνωστές εισβολές και δεν μπορεί να ανιχνεύει άγνωστες εισβολές. Η ανίχνευση ανωμαλιών ανιχνεύει άγνωστες εισβολές, αλλά έχει ένα χαμηλό ποσοστό ανίχνευσης και υψηλή υπολογιστική πολυπλοκότητα. Είναι επίσης σημαντικό σταδιακά να μάθει νέες εισβολές. Για να αποκτήσει ανίχνευση εισβολής με προαναφερθείσες τεχνικές, προτείνετε ένα σταδιακό υβριδικό σύστημα που συνδυάζει την σταδιακή ανίχνευση εισβολή κακής χρήσης και σταδιακή ανίχνευση ανωμαλιών. Το πλαίσιο για το προτεινόμενο υβριδικό σύστημα ανίχνευσης εισβολής φαίνεται στο Σχήμα.

Το προτεινόμενο πλαίσιο χωρίζεται σε δύο φάσεις: online φάση και off-line φάση. Η κατάχρηση ανίχνευσης εισβολής στοιχείων χρησιμοποιούνται για την on-line φάση. Μπορεί να μάθει νέα κατηγορία των εισβολών που δεν υπάρχουν σε προηγούμενα δεδομένα που χρησιμοποιούνται για την εκπαίδευση των υπαρχόντων ταξινομητών. Με άλλα λόγια, μπορεί να μάθει νέα κατηγορία των εισβολών σε επίβλεψη λειτουργίας. Είναι επίσης κατάλληλο για την εκμάθηση γνωστών εισβολών στην on-line λειτουργία, λόγω της χρήσης συνόλου των αδύναμων ταξινομητών με χαμηλότερη υπολογιστική πολυπλοκότητα.

Στο off-line τμήμα του πλαισίου μας, χρησιμοποιούμε σε απευθείας σύνδεση k-μέσος αλγόριθμος. Μπορεί να αναγνωρίσει νέες άγνωστες εισβολές και μπορεί σταδιακά να μάθει νέες περιπτώσεις των δεδομένων. Τα νέα αναγνώρισαν εισβολές από ανίχνευση ανωμαλίας στοιχείων που πρέπει να ισχύει στη κατάχρηση εισβολής ανίχνευσης στοιχείου στην επόμενη φάση εκμάθησης. Συνεπώς, θα πρέπει να καθορίσει την κατηγορία τύπου των νέων εισβολών. Για το λόγο αυτό, ένα άλλο στοιχείο χρησιμοποιείται για τον προσδιορισμό της κατηγορίας τύπου των νέων διεισδύσεων. Αυτό το στοιχείο είναι προαιρετικό και μπορεί να γίνει από το διαχειριστή του συστήματος. Οποιαδήποτε επιτήρηση ή ανεπιτήρητη συσσώρευση αλγορίθμου μπορεί να χρησιμοποιηθεί για αυτό το στοιχείο. Στο πείραμά μας, για λόγους απλότητας, αυτόματα καθορίζεται ο τύπος κλάσης εισβολών που εντοπίστηκαν από ανίχνευση ανωμαλιών στοιχείου.[4]

4.1.5. Κίνητρα για υβριδική προσέγγιση

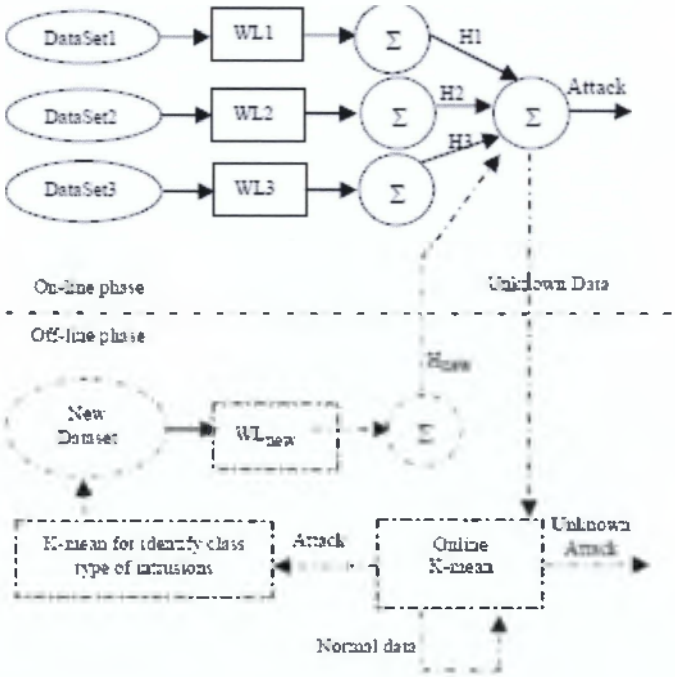
Ο στόχος του έργου είναι η υλοποίηση κατάλληλων μοντέλων που μπορούν να λειτουργήσουν αποτελεσματικά σε πραγματικό χρόνο. Κατά την εφαρμογή ενός μοντέλου σε ένα σύστημα πραγματικού χρόνου και αυτό με τη σειρά του είχε τις ακόλουθες παγίδες.

Διαχωρισμός πηγής από εισερχόμενη κίνηση είναι το πρώτο και κύριο βήμα στο σχεδιασμό. Με αυτό τον τρόπο, το μοντέλο παρακολουθεί όλες τις εισερχόμενες διευθύνσεις IP. Αλλά μετά, το πρόβλημα των πλαστογραφήσεων IP διευθύνσεων μπορεί να φορολογήσει προτεινόμενο μοντέλο. Ας υποθέσουμε ότι ένα εισερχόμενο πακέτο έχει πλαστή διεύθυνση IP. Ο διακομιστής απαντά σε αυτό και παραχωρεί πόρους για αυτήν την διεύθυνση IP. Είναι εξαιρετικά απίθανο ότι η σύνδεση που πραγματοποιείται από μια πλαστή διεύθυνση IP να προχωρήσει περαιτέρω. Αυτό θα κάνει τον διακομιστή να περιμένει μέχρι να λήξη ο χρόνος περιόδου και να επαναληφθεί από επιτιθέμενους και να οδηγήσει σε εξάντληση των πόρων ενός διακομιστή.

Το δεύτερο ζήτημα που πρέπει να εξεταστεί είναι η τυπική διάρκεια μιας σύνδεσης. Τα στοιχεία dapra που χρησιμοποιούνται για την εκπαίδευση και εξέταση ενός μοντέλου έχει πληροφορίες για ολόκληρες συνδέσεις. Αλλά στην πραγματικότητα,

δεν υπάρχει κανένας τρόπος να πει ότι η σύνδεση θα τελείωνε. Οι υπολογισμοί που εκτελούνται έχει πλήρη από άκρη σε άκρη σύνδεση δεδομένων, η οποία είναι εντελώς αδύνατο στην πραγματικότητα. Αν αυτό το μοντέλο έπρεπε να εφαρμοστεί σε ένα διακομιστή, τότε ο διακομιστής θα έπρεπε να είχε ξεχωριστή ενδιάμεση μνήμη για κάθε εισερχόμενη νέα σύνδεση. Αυτό και πάλι θα καταλήξει στη χρήση όλων των διαθέσιμων ενδιάμεσων μνημών του διακομιστή για την αποθήκευση πακέτων. Δεν μπορεί να αποφασίσει για πόσο διάστημα μια ενδιάμεση μνήμη είναι σε διαθέσει, δεδομένου ότι δεν γνωρίζουμε το μήκος της κάθε σύνδεσης.

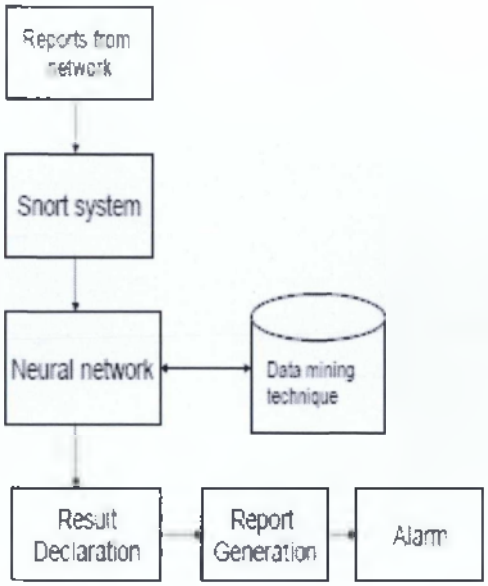
Προαναφερθέντα μειονεκτήματα εμποδίζουν το HMM με βάση το μοντέλο από το να υλοποιηθεί ως αυτόνομη συσκευή για την ασφάλεια ενός διακομιστή.[3]



Εικόνα 15: Υβριδική προσέγγιση

4.1.6. Υβριδικό μοντέλο που χρησιμοποιεί Snort

Υβριδικό μοντέλο είναι ο συνδυασμός του συστήματος snort, νευρωνικών δικτύων, και περιλαμβάνει τεχνικές εξόρυξης δεδομένων. Αυτό βελτιώνει την τρέχουσα ασφάλεια του συστήματος.



Εικόνα 16: Υβριδικό μοντέλο με χρήση Snort

Τα βήματα που περιλαμβάνονται είναι:

Αναφορές από το δίκτυο (Reportsfromnetwork): Το δίκτυο συλλέγει την κυκλοφορία του αισθητήρα από το επίπεδο των φύλλων, όταν λαμβάνει τις αναφορές από το χαμηλότερο επίπεδο. Αυτές έχουν αναπτυχθεί σε ένα δίκτυο ή σε μια συσκευή για τη συλλογή δεδομένων. Παίρνουν τη συμβολή από διάφορες πηγές, συμπεριλαμβανομένων των πακέτων δικτύου, τα αρχεία καταγραφής, και τα ίχνη κλήση συστήματος. Η είσοδος συλλέγεται, οργανώνεται και μετά προωθείται σε έναν ή περισσότερους αναλυτές.

Σύστημα Snort (SnortSystem): Ανιχνεύει εισβολές από την πρώτη ανάλυση κίνησης δικτύου για να εξαγάγει ένα επίπεδο εφαρμογής σημασιολογίας και μετά εκτέλεση της εκδήλωση προσανατολισμένη ανάλυσης που συγκρίνει τη δραστηριότητα με τα θεωρούμενα προβληματικά σχέδια.

Νευρωνικά εξόρυξης δικτύου και δεδομένων (Neuralnetworkanddatamining): Χρήση ταξινόμησης νευρωνικών δικτύου με συνδυασμό της τεχνικής κατάχρησης που αποτελεσματικά και γρήγορα ταξινομήθηκαν τα ακόλουθα πακέτα δικτύου σε

σχέση με την επίθεση σχεδίου που έχει εκπαιδευτεί να αναγνωρίζει. Αυτή είναι μια τροφοδοσία προς τα εμπρός δικτύου το οποίο χρησιμοποιεί εποπτευόμενη εκπαίδευση, και η οποία:

- Μπορεί να εκπαιδευτεί γρήγορα,
- Μπορεί να εκπαιδευτεί σταδιακά,
- Αφού εκπαιδευτεί, μπορεί να εκτελέσει γρήγορες και ακριβείς ταξινομήσεις των εισροών της.

Χρησιμοποιείται και εκπαιδεύεται για να βρίσκει πληροφορίες χρησιμοποιώντας τα στοιχεία τεχνική εξόρυξης από τα παλαιότερα αποθηκευμένα δεδομένα.

Αποτέλεσμα δήλωσης (ResultDeclaration): Σε αυτό το βήμα το αποτέλεσμα στο συμπέρασμα και το αποτέλεσμα περαιτέρω περασμάτων στο επόμενο επίπεδο για την αποθήκευση των αποτελεσμάτων για μεταγενέστερη χρήση.

Αναφορά δημιουργίας (ReportGeneration): Αναφορά παράγεται για να δώσει τις πληροφορίες σχετικά με τις επιθέσεις. Οι αναφορές αυτές μετά στέλνονται στο διαχειριστή ασφάλειας.

Συναγερμός (Alarm): Αν εντοπίσει μια εισβολή, τότε αυξάνει τον κώδωνα του κινδύνου. Ηχεί ο συναγερμός όταν διαπιστωθεί η εισβολή σε ένα σύστημα.[16]

4.1.7. Υβριδική σάρωση

Η μείωση των θυμάτων που πρόκειται να σαρωθούν από μία βάση δεδομένων μπορεί να οδηγήσει στο να χαθούν αρκετά ευάλωτα συστήματα τα οποία δεν είναι προσβάσιμα από παντού. Για να λυθεί αυτό το πρόβλημα, ο επιτιθέμενος μπορεί να συνδυάσει τη μέθοδο routablescan με τη τυχαία σάρωση, σε μία μετέπειτα φάση της διάδοσης (όταν έχουν σαρωθεί ήδη οι περισσότερες διευθύνσεις) ώστε να μολύνει περισσότερα συστήματα. Η μέθοδος routablescan είναι ένα είδος στρατηγικής όπου το δικτυακό worm σαρώνει επιλεκτικά IP διευθύνσεις με βάση πληροφορίες δρομολόγησης που έχει συλλέξει από ένα δίκτυο

Αυτή η μέθοδος σάρωσης ονομάζεται υβριδική. Το πλεονέκτημα αυτής της μεθόδου είναι ότι αν και η διάδοση μπορεί να έχει ανιχνευτεί, η υβριδική σάρωση μπορεί να

χρησιμοποιηθεί για να μολύνει περισσότερα συστήματα καθώς είναι ήδη αργά για αποτελεσματική άμυνα.

Λαμβάνοντας υπόψη το γεγονός ότι ένας μεγάλος αριθμός από συστήματα χρησιμοποιούν ιδιωτικές διευθύνσεις, και είναι κρυμμένα και προστατευμένα πίσω από συστήματα gateway, καλύτερη απόδοση μπορεί να επιτευχθεί αν αυτές οι διευθύνσεις μπορούν να σαρωθούν με περισσότερη δύναμη. Επιπρόσθετα, κάθε κάρτα διασύνδεσης ενός δικτύου ενός θύματος θα μπορούσε να χρησιμοποιηθεί ώστε η σάρωση του worm να φθάσει σε περισσότερα υποδίκτυα.

4.1.8. Υβριδικά Firewalls

Τα υβριδικά firewalls συνδυάζουν ελέγχους επιπέδου δικτύου και εφαρμογής. Τα λαμβανόμενα πακέτα υπόκεινται πρώτα σε έλεγχο επιπέδου δικτύου, συνεπώς είτε απορρίπτονται, είτε προωθούνται προς τον προορισμό τους. Επίσης μπορούν σταλούν σε πληρεξούσια υπηρεσία για περαιτέρω επεξεργασία. Τα υβριδικά firewalls έχουν πολύ καλό επίπεδο ασφαλείας αλλά έχουν αυξημένο κόστος υλοποίησης. Υπάρχουν τρεις βασικές αρχιτεκτονικές υβριδικών αναχωμάτων ασφάλειας: Dual-homedGateway, ScreenedHost και ScreenedSubnet.[18]

4.2. Αρχιτεκτονική υβριδικούIDS

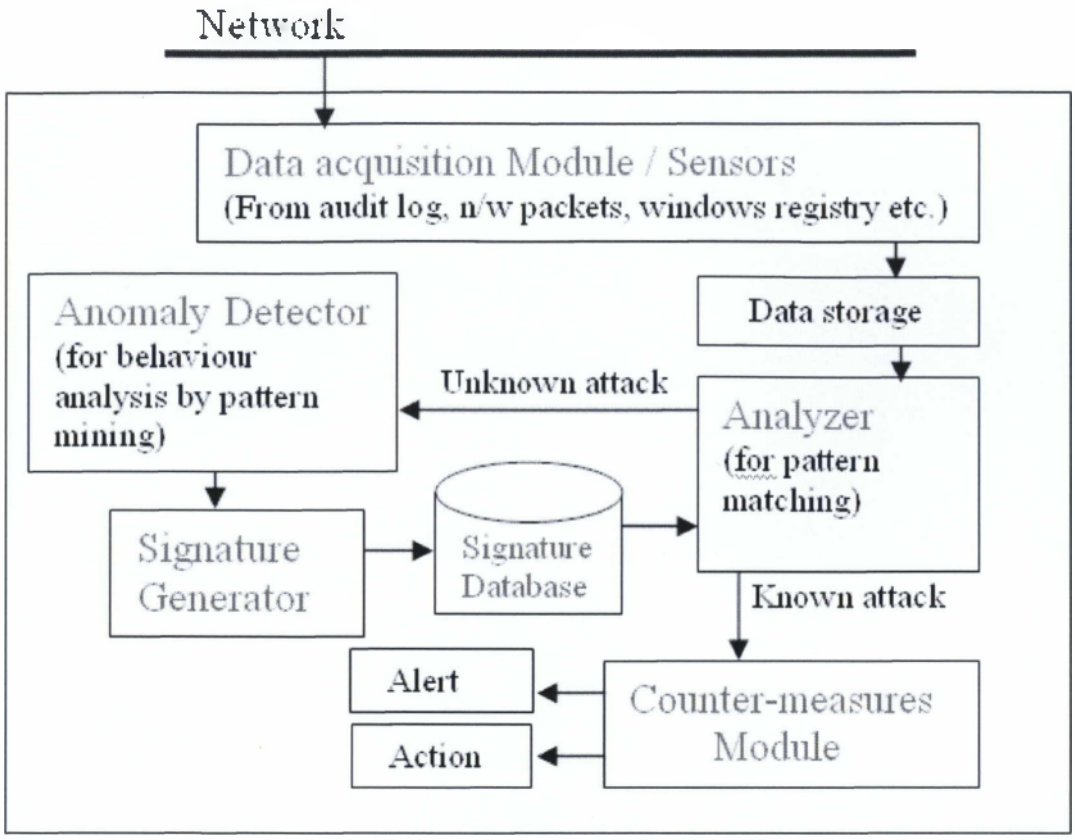
Τα υβριδικά συστήματα IDS αποτελούνται από έξη μέρη:

- Dataacquisitionmodule (Απόκτηση δεδομένων εξαρτημάτων)
- Signaturedata-based (Βάση δεδομένων υπογραφών)
- Analyzer (Αναλυτής)
- Anomalydetector (Ανιχνευτής ανωμαλιών)
- Signature generator (Κύκλωμα υπογραφών)
- Counter-measure module (Ενότηταναντιμέτρων)

Το Dataacquisitionmodule έχει πολλαπλούς αισθητήρες. Οι αισθητήρες τοποθετούνται είτε σε ατομική υποδοχή ή σε συγκεκριμένο τμήμα του δικτύου.Αισθητήρες που τοποθετούνται σε ατομικά συστήματα παρατηρούν τα

πακέτα που εισέρχονται και εξέρχονται από την υποδοχή. Αισθητήρες που τοποθετούνται σε ένα συγκεκριμένο τμήμα του δικτύου διαβάζουν τα πακέτα που περνούν μέσα και έξω από κάθε τμήμα. Οι αισθητήρες πρέπει να τοποθετούνται σε χώρους όπου θα είναι σε θέση να συλλάβουν όλα τα πακέτα που εισέρχονται και εξέρχονται από μια υποδοχή ή τμήμα του δικτύου. Αισθητήρες που τοποθετούνται σε τμήματα του δικτύου δεν έχουν πάντα τη δυνατότητα, εάν το επίπεδο της κυκλοφορίας γίνεται πάρα πολύ βαριά, για να συλλάβουν κάθε πακέτο. Επανατοποθέτηση των αισθητήρων σε κάθε υποδοχή του δικτύου θα βελτιώσει την ακρίβεια, ακόμη και αν η προσπάθεια για την εγκατάσταση τους μπορεί να είναι σημαντική. Το σημαντικό πράγμα είναι να είναι σε θέση να συλλάβει όλα τα πακέτα, έτσι ώστε κανένας να μην μπορεί να παρακάμψει ενδεχομένως τα IDS. Για τους σκοπούς μας χρησιμοποιούμε Snort για το λειτουργικό σύστημα των Windows χρησιμοποιώντας WinPcap.

Το Signaturedata-based επιτρέπουν τα IDS για να υπάρχει μια σειρά από υπογραφές, κριτήρια ή κανόνες εναντίον όποιον θα μπορεί να συγκρίνει τα πακέτα που περνούν μέσα από τον αισθητήρα. Η βάση δεδομένων των υπογραφών πρέπει να εγκατασταθεί μαζί με το λογισμικό και το υλικό IDS. Αφού η βάση δεδομένων υπογραφών είναι σε θέση, οι αισθητήρες της απόκτησης δεδομένων εξαρτημάτων συγκεντρώνουν τα δεδομένα από την ανάγνωση πακέτων από το δίκτυο και τα επανασυναρμολογούν. Εξίσου τα πακέτα από το δίκτυο μπορούν να φτάσουν εκτός λειτουργίας, ή μπορούν να αντιγραφούν. Επιπλέον, τα πακέτα φθάνουν σε υψηλή ταχύτητα επομένως η αποθήκευση δεδομένων είναι υποχρεωτικό για την αποθήκευση των πακέτων.



Εικόνα 17: Αρχιτεκτονική υβριδικού IDS

Το Analyzer εξάρτημα συγκρίνει τα πακέτα τα παρατηρεί με τις υπογραφές ή τους κανόνες φυσιολογικών προτύπων συμπεριφοράς αποθηκεύοντας στη βάση δεδομένων υπογραφών χρησιμοποιώντας μοτίβο κατάλληλου αλγόριθμου. Χρησιμοποιούμε το γνωστό Aho-Corasick αλγόριθμο για την εκτέλεση κατάλληλων σχεδίων. Αν ο αναλυτής διαπιστώσει οποιοδήποτε αγώνα στη συνέχεια στέλνει κατάλληλο μήνυμα προειδοποίησης για τις γνωστές επίθεση στη μονάδα Counter-measuremodule. Επίσης εισάγει καταχώρηση στο αρχείο καταγραφής για το συμβάν που προκάλεσε την προειδοποίηση. Αν ο αναλυτής δεν βρει κανένα αγώνα στη συνέχεια στέλνει τα δεδομένα προς τον ανιχνευτή ανωμαλιών για την εύρεση ανωμαλιών που χρησιμοποιούν σχέδιο τεχνικής εξόρυξης. Εάν ο ανιχνευτής ανωμαλιών διαπιστώσει οποιαδήποτε ανωμαλία στη συνέχεια στέλνει το κατάλληλο μήνυμα στο κύκλωμα υπογραφών. Εδώ το κύκλωμα υπογραφών δημιουργεί κανόνες ή υπογραφές και κάνουν νέες εγγραφές στη βάση δεδομένων υπογραφών.

Όταν το Counter-measuremodule λάβει το μήνυμα ειδοποίησης γνωστών επιθέσεων από τον αναλυτή, ειδοποιεί το διαχειριστή σε έναν από τους πολλούς τρόπους που ο διαχειριστής έχει ρυθμίσει εκ των προτέρων . Η μονάδα μπορεί να εμφανίσει ένα

pop- up παράθυρο ή στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου με το ξεχωριστό χαρακτηριστικό, για παράδειγμα. Εκτός από την αυτόματη απάντηση αποστέλλεται στον διαχειριστή, το εξάρτημα που μπορεί να ρυθμίσει ώστε να αναλάβει δράση την ίδια στιγμή που ένα προειδοποιητικό μήνυμα έχει ληφθεί. Τυπικές δράσεις είναι οι εξής: i) Συναγερμός, στην οποία ένας συναγερμός αποστέλλεται στον διαχειριστή, ii) Drop, στην οποία το πακέτο πέσει χωρίς μήνυμα λάθους αποστέλλεται στον υπολογιστή καταγωγής και iii) επαναφορά, η οποία καθοδηγεί το IDS να σταματήσει και κάνει επανεκκίνηση της κυκλοφορίας στο δίκτυο και συνεπώς να σταματήσει ιδιαίτερα σοβαρές επιθέσεις. Το εξάρτημα χρησιμοποιείται επίσης από το διαχειριστή του δικτύου για να αξιολογήσει το μήνυμα ειδοποίησης και να πάρει τις κατάλληλες ενέργειες όπως ρίψη ένας πακέτου ή το κλείσιμο μιας σύνδεσης. Ο διαχειριστής μπορεί να προβλέψει αν χρειάζεται να τελειοποιήσει τη βάση δεδομένων υπογραφών στο λογαριασμό του για καταστάσεις που φαίνονται στην IDS εισβολών, αλλά στην πραγματικότητα είναι νόμιμη κίνηση. Για παράδειγμα, η προσαρμογή θα μπορούσε να γίνει για να επιτρέψει την κυκλοφορία που θα μπορούσαν αλλιώς να δει από το τείχος προστασίας ως ύποπτο, όπως μια ευπάθεια σάρωση γίνεται από συσκευή σάρωσης που βρίσκεται σε μια συγκεκριμένη διεύθυνση IP . Τα IDS θα μπορούσαν να ρυθμιστούν ώστε να προσθέσουν έναν κανόνα που αλλάζει την ενέργεια που πραγματοποιείται από τα IDS ως απάντηση στην κίνηση από τη διεύθυνση IP από alarmtodrop.[1]

4.2.1. Μοναδικά χαρακτηριστικά των υβριδικών IDS

Τα ακόλουθα είναι ο κατάλογος των μοναδικών χαρακτηριστικών των υβριδικών IDS.

- Είναι εύκολο να εγκατασταθεί και να ρυθμιστεί.
- Είναι προσαρμοστικό στη φύση και προσαρμόζει τις αλλαγές στην συμπεριφορά του χρήστη και του συστήματος.
- Τρέχει συνεχώς με την ελάχιστη ανθρώπινη επιτήρηση. Δημιουργεί τις υπογραφές των νέων επιθέσεων.
- Σχεδιασμός των υβριδικών IDS καθιστά ανεκτική σε σφάλματα, έτσι ώστε θα είναι σε θέση να ανακάμψει από τις συντριβές. Θα είναι σε θέση να πάρει

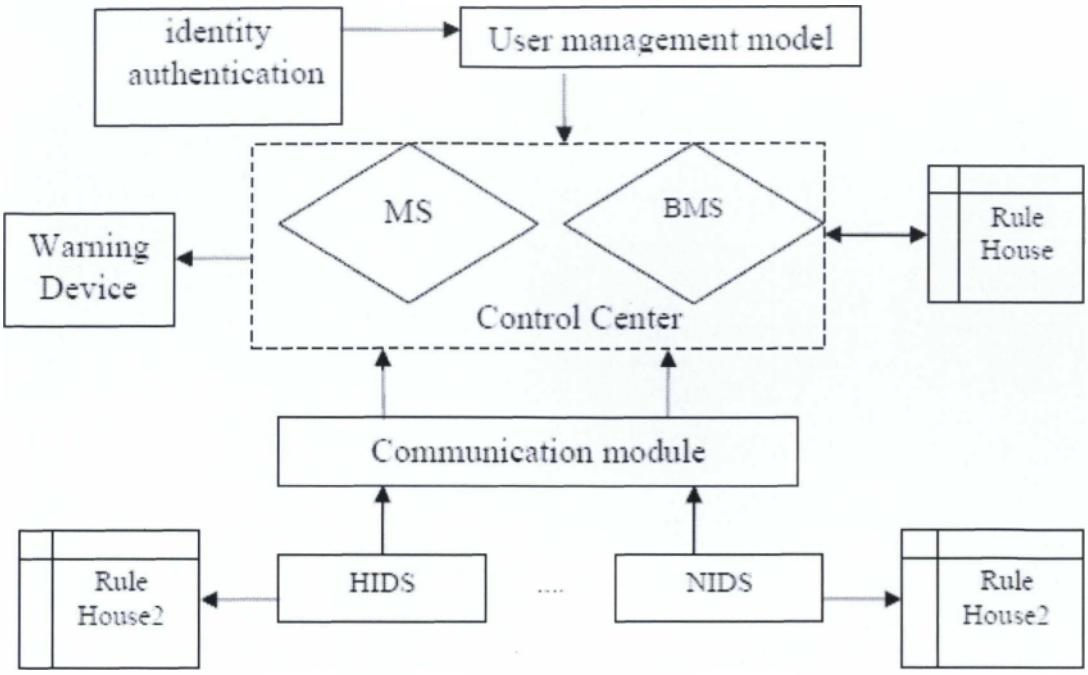
προηγούμενη κατάσταση και να επαναλάβει τη λειτουργία του χωρίς καμία αρνητική επίδραση.

- Είναι σε θέση η ίδια να ελέγχει και να εντοπίζει τις επιθέσεις σε αυτό.
- Θα καταναλώνουν λιγότερη μνήμη για να λειτουργήσει. Μπορεί να τρέξει με λιγότερη επιβάρυνση στα συστήματα όπου είναι εγκατεστημένα.
- Θα είναι ακριβής και με αυτόν τον τρόπο θα υπάρχει λιγότερος αριθμός των ψευδών θετικών και ψευδών αρνητικών αποτελεσμάτων.[1]

4.3. Σχεδιασμός NIDS και HIDS υβριδικής ανίχνευσης εισβολής

Πολλά IDS τείνουν να χρησιμοποιούν μεθόδους ανίχνευσης με βάση το δίκτυο ή με βάση υποδοχής μεθόδους ανίχνευσης για την επίτευξη της ασφάλειας. Ωστόσο, η ανεπάρκεια των HIDS και NIDS: στην αντιμετώπιση του πολυσύνθετου περιβάλλοντα δικτύου, οι ελλείψεις του NIDS είναι ότι η παρακολούθηση της ποσότητας των δεδομένων είναι πολύ μεγάλη και δεν μπορεί να συνδυαστεί με τις λειτουργικές δυνατότητες του συστήματος για να κριθεί με ακρίβεια η συμπεριφορά του δικτύου. Επιπλέον, το NIDS δεν θα μπορεί να συλλέγει σε πραγματικό χρόνο όλα τα πακέτα δεδομένων. Το HIDS περιορίζεται από το περιβάλλον ανάπτυξης, στηρίζει μόνο μία ασφάλεια υποδοχής, έλλειψη cross-platform, κακή φορητότητα, έτσι περιορίζει το πεδίο εφαρμογής και την εισβολή στο πρωτόκολλο του δικτύου.

Για αυτά τα ελαττώματα, κατασκευάστηκαν HIDS και NIDS υβριδικής ανίχνευσης εισβολής μοντέλου του συστήματος, όπως φαίνεται στο Σχήμα 18:



Εικόνα 18: Σχεδίαση υβριδικών NIDS και HIDS

Το κέντρο ελέγχου χρησιμοποιείται κυρίως για να καθορίσει αν οι εξελιγμένες επιθέσεις εισβολής, του κύριου συστήματος και άλλες επικοινωνίες δικτύων για την ανταλλαγή πληροφοριών, τους κανόνες ενημέρωσης, κανόνες πληροφορήσεις εργασιών με βάση δεδομένων, κάνουν την κατάλληλη προειδοποίηση. Περιλαμβάνει ένα ειδικό σύστημα (MasterSystem) και βασισμένο στο σύστημα ειδικό (BasedMasterSystem), το ειδικό είναι ο πυρήνας του συστήματος, το δεύτερο σύστημα ελέγχου είναι ένα αντίγραφο ασφαλείας του κύριου συστήματος, αποτρέποντας τον έλεγχο ειδικής επίθεση κέντρου όταν δεν λειτουργεί, αντικαθίσταται το ειδικό σύστημα ελέγχου που ολοκληρώνει την εργασία.

Η μονάδα επικοινωνίας γίνεται μέσω του μηχανισμού SOCKET στο κέντρο ελέγχου και HIDS (NIDS) για την ανταλλαγή πληροφοριών. Τα στοιχεία επικοινωνίας θα πρέπει να έχουν βασικές λειτουργίες: την παράδοση των μηνυμάτων, να λαμβάνει το μήνυμα και το μήνυμα.

Κανόνας (1) εάν ανιχνευθεί στα πακέτα με υπογραφές επίθεσης, αποθηκεύονται στη βάση δεδομένων, ανάλυση συστημάτων, στατιστικής δειγματοληψίας ή στατιστικές μονάδες ανάλυσης. Κανόνας (2) κανόνες αποθήκευσης των χαρακτηριστικών της εισβολής ή εισβολής όπως ανίχνευση εισβολής ανάλυσης μοντέλου δεδομένων αν υπάρχουν εξαιρέσεις που βασίζονται στη συσκευασία.

Ο χρήστης διαχείρισης μοντέλου πρέπει να περάσει πιστοποίηση ταυτότητας, και μετά τη διαχείριση ολόκληρου του συστήματος, συμπεριλαμβανομένης της βάσης κανόνα για την αναβάθμιση και βελτίωση, η διαχείριση καταγραφής του συστήματος, ανάλυσης και άλλες λειτουργίες.[19]

4.3.1. Υβριδικό IDS: H-Snort

Πρέπει να σχεδιαστεί ένας προ-επεξεργαστής για να επιτρέπει την ανίχνευση ανωμαλιών που θα εξελίξει το Snort σε ένα υβριδικό σύστημα. Το σύστημα αυτό, που ονομάζεται H-Snort πληροί τις ακόλουθες προϋποθέσεις:

- Τα μοντέλα κίνησης δικτύου έχουν υψηλό επίπεδο.
- Αποθηκεύει τις πληροφορίες σε μια βάση δεδομένων, για να διαμορφώσει την φυσιολογική συμπεριφορά του συστήματος.
- Είναι τελείως διαμορφωμένο και επιτρέπει τη ρύθμιση της ευαισθησίας του συστήματος για την πρόληψη ψευδών συναγερμών.
- Έχει δύο φάσεις χειρισμού: εκπαίδευση και την ανίχνευση ανωμαλιών.
- Είναι συμπληρωμένο με ένα δικτυακό τόπο που επιτρέπει στο χρήστη να διαχειρίζεται και να παρατηρεί την απόδοση του δικτύου.

Το σύστημα Snort έχει επεκταθεί με την προσθήκη ανίχνευσης ανωμαλίας προ-επεξεργαστή που έχουν πρόσβαση σε μια βάση δεδομένων MySQL, όπου είναι το κεντρικό σύστημα διαμόρφωσης, στατιστικά στοιχεία και ανωμαλίες που ανιχνεύθηκαν από το σύστημα. Το σύστημα ολοκληρώνεται από μια ιστοσελίδα που εμφανίζει την κατάσταση του συστήματος (κίνηση στο δίκτυο, εντοπίζονται ανωμαλίες, κ.λπ.) και ότι, επίσης, σας επιτρέπει να ρυθμίσετε εύκολα το σύστημα.[21]

Κεφάλαιο 5: Σύγκριση και υλοποίηση ανίχνευσης και πρόληψης εισβολών

5.1. Εισαγωγή

Παρά το γεγονός ότι η ανωνυμία και η προστασία της ιδιωτικής ζωής είναι μόνο ένα μικρό μέρος αυτού που σήμερα ονομάζεται υπολογιστής ή ασφάλεια των δικτύων, διαδραματίζει ζωτικό ρόλο στην προστασία των δεδομένων. Υπάρχουν μερικά ζητήματα που η κρυπτογράφηση δεδομένων σε δημόσια δίκτυα δεν είναι αρκετά. Μεταξύ αυτών είναι σημαντικά πεδία, όπως η ελευθερία του λόγου, τις εκλογές, την υγειονομική περίθαλψη και τα συστήματα κοινωνικής καθοδήγησης. Το απλό γεγονός της ανταλλαγής πακέτων δεδομένων με ορισμένους φορείς μπορεί να είναι ήδη ενδιαφέρον σε τρίτους, δηλαδή οι άνθρωποι θα ήθελαν να χρησιμοποιήσουν αυτά τα συστήματα ανώνυμα.

Αντίθετα τα περισσότερα πρωτόκολλα δικτύου, και ιδίως το πρωτόκολλο TCP / IP, δεν έχουν σχεδιαστεί για ανώνυμη μεταφορά δεδομένων. Οποιοσδήποτε κατά μήκος της διαδρομής του πακέτου μέσω ενός δικτύου μπορεί να παρατηρήσει την προέλευση και τον προορισμό του πακέτου αυτού, ακόμη και αν το ωφέλιμο φορτίο είναι κρυπτογραφημένη. Ως εκ τούτου, ο Chaumet αϊ. έχει προτείνει πρωτόκολλα ανωνυμίας που παρέχει προστασία έναντι αυτού του είδους των υποκλοπών σε κλειστά περιβάλλοντος [Cha81, Cha88, CGKS95, CB95].

Η ανάγκη για τη μέτρηση της απόδοσης των εφαρμογών ανωνυμίας εμφανίστηκε με την ανάπτυξη των εφαρμογών που επέτρεψε ανώνυμες ηλεκτρονικές συναλλαγές, παραδείγματος χάριν δυσκολία εντοπισμού email, ηλεκτρονική ψηφοφορία, ανώνυμα ecoins ή ενίσχυση απομόνωσης πλοήγηση στο διαδίκτυο.

Τα ερευνητικά ερωτήματα που προέκυψαν ήταν: πώς μπορεί να μετρηθεί η ανωνυμία; Πώς μπορεί δύο διαφορετικά συστήματα ανωνυμίας να συγκριθούν; Είναι ένα γενικό μέτρημα ανωνυμίας που μπορεί να εφαρμοστεί σε οποιοδήποτε σύστημα ανωνυμίας εκεί; Πώς μπορούμε να αξιολογήσουμε την αποτελεσματικότητα των διαφόρων επιθέσεων στο σύστημα ανωνυμίας; Πώς μπορούμε να εκτιμήσουμε τις απώλειες και τα κέρδη στην ανωνυμία; Πώς μια μετρική ανωνυμία αντικατοπτρίζει τη μερική ή στατιστική πληροφορία που συχνά επιτυγχάνεται μέσω ενός αντιπάλου; Οι μετρικές που περιγράφονται εδώ παρέχουν απαντήσεις σε αυτά τα ερωτήματα.

Οι μετρήσεις ανωνυμίας που παρουσιάζονται μπορούν να εφαρμοστούν σε συγκεκριμένα συστήματα, αντιπάλους, και συνθήκες. Οι μετρήσεις αυτές δίνουν ένα μέτρο του μεγέθους και ικανότητα να διακρίνουν το σύνολο των θεμάτων που ενδέχεται να σχετίζονται με μια συγκεκριμένη συναλλαγή, και επιτέθηκε από ένα συγκεκριμένο αντίπαλο. Για να πάρετε μια ιδέα απόδοσης μιας εφαρμογής ανωνυμίας υπό διαφορετικές συνθήκες, πολλαπλές μετρήσεις ανωνυμιών πρέπει να γίνουν και να αναλυθούν.

Πληροφορίες θεωρητικών μετρήσεων μπορούν να εφαρμοστούν σε ένα ευρύ φάσμα συστημάτων ανωνυμίας. Συνεπώς είναι σημαντικό να κατανοηθούν οι έννοιες πίσω από τη βάση εντροπία μετρήσεων ανωνυμιών, προκειμένου να εφαρμοστούν και να ερμηνευτούν σωστά σε συγκεκριμένα σενάρια. Οι μετρήσεις θα πρέπει να προσαρμοστούν στο σύστημα ανωνυμίας υπό μελέτη, και ο υπολογισμός των κατανομών πιθανότητας που οδηγούν σε ουσιαστικές μετρικές τιμές δεν είναι πάντα προφανής.

Η εργασία αυτή επικεντρώνεται στην ανάλυση της ισχύος των εν λόγω πρωτοκόλλων σε ένα ανοικτό σύστημα, όπως το διαδίκτυο [GRS 96, GT 96, RR98, KEB 98, KBS02]. Ειδικότερα, θα διερευνηθεί πόσο καιρό μπορούν να κρύψουν τις επικοινωνίες του χρήστη από ένα παθητικό εισβολέα.

Η πρώτη συμβολή της παρούσας εργασίας είναι μια νέα επίθεση που κάνει επίσης χρήση των παρατηρήσεων κίνησης του δικτύου χωρίς να παρεμβαίνει με την κίνηση του δικτύου σε κάθε είδους. Με την αναζήτηση για τα συνολικά χτύπημα παρατηρήθηκαν ότι ο νέος αλγόριθμος κάνει τη δουλειά πιο γρήγορα, δηλαδή χρειάζεται λιγότερη παρατήρηση από κάθε άλλη επίθεση γνωστή σε εμάς. Καλούμε τη νέα επίθεση συνολικό χτύπημα επίθεσης ή HS-επίθεση. Ωστόσο, αυτό απαιτεί τη λύση ενός NP-hard πρόβλημα, δηλαδή το ελάχιστο συνολικό χτύπημα προβλήματος.

Έχουμε χαλαρώσει την αυστηρή προσέγγιση του ελάχιστου συνολικού χτυπήματος χρησιμοποιώντας τους πιο συχνούς υποψήφιους. Καλούμε αυτή την επίθεση ως στατιστικό ελάχιστο συνολικό χτύπημα επίθεσης ή SHS-επίθεση. Αυτή η επίθεση δεν στηρίζεται με επίλυση NP-hard προβλήματα. Επίσης είναι πολύ εύκολη στην ανάπτυξη και μπορεί να εφαρμοστεί σε καταστάσεις που είναι πολύ πέρα από εφικτή HS-επίθεσης.

Αλλά το πλεονέκτημα αυτό έρχεται με ένα μειονέκτημα: ο κίνδυνος σφαλμάτων. Οι λύσεις που υιοθέτησε η SHS-επίθεση είναι προσεγγιστικές και συνεπώς αντιτίθεται σε πιθανά σφάλματα. Παραθέτουμε ορισμένα πιθανά στατιστικά σφάλματα και προτείνουμε στρατηγικές που μπορούν να εφαρμοστούν για τη μείωση του σφάλματος σε οποιαδήποτε αυθαίρετο μέτρο.

Τρίτη συμβολή μας είναι μια μέθοδος βελτίωσης. Θα δείξουμε πώς η προσέγγιση μπορεί να χρησιμοποιηθεί για να δείξει είτε την ορθότητα του εαυτού του ή να δώσει μια ιδέα για το πώς να αναζητήσουν περισσότερες πληροφορίες στις επερχόμενες παρατηρήσεις. Ιδιαίτερα το έργο της FredmanKhachiyan μπορεί να χρησιμοποιηθεί για μεγάλο πλεονέκτημα. Καλούμε αυτή την επίθεση HS *-επίθεση, δεδομένου ότι είναι ακριβώς όπως την HS-επίθεση και μπορεί να χρησιμοποιήσει τις στατιστικές ιδιότητες της SHS-επίθεση, αλλά απαιτεί περισσότερες παρατηρήσεις.[5][6]

5.2. Καθορισμός της ανωνυμίας

Πριν από την ποσοτικοποίηση της ανωνυμίας, ένας λειτουργικός ορισμός για τον όρο της ανωνυμίας ήταν απαραίτητος. Ο Pfitzmann και ο Hansen όρισαν την ανωνυμία ως η κατάσταση του να μην είναι αναγνωρίσιμα μέσα σε ένα σύνολο θεμάτων, το σύνολο της ανωνυμίας. Ο ορισμός αυτός, προτάθηκε για πρώτη φορά το έτος 2000, έχει υιοθετηθεί το μεγαλύτερο μέρος της βιβλιογραφικής ανωνυμίας.

Σύμφωνα με τον ορισμό της ανωνυμίας από τους Pfitzmann-Hansen, τα άτομα που μπορεί να σχετίζονται με μια ανώνυμη συναλλαγή δεν συνιστά την ανωνυμία για τη συγκεκριμένη συναλλαγή. Ένα θέμα φέρνει στην πράξη ανώνυμα, αν δεν μπορούν να διακριθούν (με αντίπαλο) από άλλα θέματα. Ο ορισμός της ανωνυμίας συλλαμβάνει την πιθανολογικές πληροφορίες που λαμβάνονται από τους αντιπάλους που προσπαθούν να προσδιορίσουν ανώνυμα θέματα.[6]

5.3. Τεχνικές ανωνυμίας

Όπως ήδη αναφέρθηκε στην εισαγωγή, υπάρχει μια σειρά από τεχνικές για την πρόληψη της ανωνυμίας ωτακουστές από την απόκτηση πληροφοριών σχετικά με την

κυκλοφορία ενός χρήστη. Δεδομένου ότι το περιεχόμενο μπορεί να είναι κρυπτογραφημένο, η εστίασή μας είναι στο στρώμα της κυκλοφορίας. Οποιοσδήποτε που μπορεί να διαβάσει ένα πακέτο μπορεί να δει την προέλευση και τον προορισμό. Οι τεχνικές ανωνυμίας προσπαθούν να αποφευχθεί αυτό.

Ως παράδειγμα: κάποιος θέλει να τοποθετήσει πολιτικά τη γνώμη του σε ένα φόρουμ στο διαδίκτυο όπου αντίθετα μέλη ανταλλάζουν πληροφορίες. Δυστυχώς, ζούμε σε μια χώρα όπου η κυβέρνηση είναι πιθανό να εντοπίζει αντιπολιτευτικά μέλη. Αν στείλουμε μόνο το κρυπτογραφημένο μήνυμα, π.χ. χρησιμοποιώντας το HTTPS, φορέα παροχής υπηρεσιών διαδικτύου (ISP) θα μπορούσε να παρατηρήσει αυτή την ενέργεια και να το αποθηκεύσει σε ένα αρχείο. Αυτό θα μπορούσε να οδηγήσει σε ένα σημείο όπου θα μπορούσαμε να πάρουμε υποψία γιατί έχει ανταλλάξει δεδομένα με κάποια οντότητα.

Για να αποφευχθεί αυτό, μπορούμε να χρησιμοποιήσουμε κάποια υπηρεσία, όπως JAP [BFK01]. Γι 'αυτό εγκαθιστάμε ένα πληρεξούσιο στον υπολογιστή μας, που κρυπτογραφεί όλες τιης κυκλοφορίες και τις στέλνει σε έναν JAP πληρεξούσιο (π.χ. Mixes [Cha81]). Ο διακομιστής αποκρυπτογραφεί τα πακέτα και τα προωθεί για λογαριασμό των χρηστών. Οποιαδήποτε δεδομένα που επιστρέφονται θα αποστείλουν στους χρήστες σχετικά με τον ίδιο τρόπο.

Συνεπώς, οποιαδήποτε κύρια στοιχεία έχουν πλέον περάσει. Αυτό που μένει είναι να στείλουμε τα δεδομένα σε ένα διακομιστή ανωνυμίας (π.χ. Mixes), η οποία από μόνη της δεν παρέχει καμία άλλη υπηρεσία από μη ανιχνεύσιμη προώθηση των πακέτων. Εξαιτίας αυτής της λειτουργικότητας ένας πιθανός εισβολέας δεν είναι σε θέση να συνδέσει ένα εισερχόμενο πακέτο σε ένα εξερχόμενο πακέτο. Χρησιμοποιώντας αυτή την υπηρεσία, είναι πέρα από κάθε υποψία ότι έχουν στείλει κάποια πακέτα στο αντιπολιτευτικό φόρουμ επειδή κάποιος από τους άλλους χρήστες να το έχει κάνει, δηλαδή και τα άλλα πρόσωπα που χτίζουν το λεγόμενο σύνολο ανωνυμίας.[5]

5.3.1. Η αντίληψη των Mix

Τα Mix συλλέγουν μια σειρά από πακέτα από διαφορετικούς χρήστες (σύνολο ανωνυμίας) και την επεξεργασία τους, έτσι ώστε κανένας συμμετέχων, εκτός από το

MIX τον εαυτό τους και τον αποστολέα του πακέτου, να συνδέετε από ένα πακέτο εισόδου σε ένα πακέτο εξόδου [Cha81]. Συνεπώς, η εμφάνιση (δηλαδή τα δυαδικά ψηφία), και η σειρά των εισερχόμενων πακέτων πρέπει να αλλάξει μέσα στο Mix. Η αλλαγή της εμφάνισης είναι μια κρυπτογραφημένη λειτουργία, η οποία συνδυάζεται με μια διαδικασία διαχείρισης και καθολική συμφωνία για επιτευχθεί η ανωνυμία:

Χρήστης πρωτοκόλλου (Userprotocol): Όλα δημιουργούνται πακέτα δεδομένων συμπεριλαμβανομένων των πληροφοριών διεύθυνσης είναι παραγεμισμένο με ίσου μήκους (συμφωνία), σε συνδυασμό με ένα μυστικό τυχαίο αριθμό RN, και με κρυπτογραφημένο το δημόσιο κλειδί του κόμβου MIX. Μια ακολουθία Mixes χρησιμοποιείται για να αυξήσει την αξιοπιστία του συστήματος.

Mix πρωτόκολλο (Mixprotocol): Το MIX συλλέγει πακέτα (που ονομάζονται batch) από διαφορετικούς χρήστες (επαλήθευση ταυτότητας), αποκρυπτογραφεί τα πακέτα με το ιδιωτικό κλειδί του, αφαιρεί το RNs, και εξάγει τα πακέτα με διαφορετική σειρά (λεξικογραφικά ταξινομημένο ή τυχαία καθυστερήσει). Επιπλέον, κάθε εισερχόμενο πακέτο πρέπει να συγκριθεί με το παλαιότερο ληφθέν πακέτο (διαχείριση: κατάστημα σε μια τοπική βάση δεδομένων), προκειμένου να απορρίψει οποιαδήποτε διπλότυπα. Κάθε MIX (εκτός από το πρώτο) πρέπει να περιλαμβάνουν μία λειτουργικότητα που εξασφαλίζει ότι κάθε λαμβανόμενο πακέτο είναι από ξεχωριστό χρήστη, επειδή μόνο το πρώτο Mix μπορεί να αποφασίσει κατά πόσον ή όχι τα πακέτα είναι από διαφορετικούς αποστολείς.

Εφαρμόζοντας αυτό το πρωτόκολλο σε κλειστούς χώρους, όπου όλα τα άτομα συμμετέχουν σε όλα τα σετ ανωνυμία, η μέθοδος MIX παρέχει πλήρη ασφάλεια. Η σχέση μεταξύ του αποστολέα και του παραλήπτη είναι κρυμμένο από μια πανταχού παρούσα εισβολέα εφ 'όσον:[6]

- Ένας ειλικρινής MIX είναι στη γραμμή των Mixes που το πακέτο διέρχεται.
- Το (α - 1) άλλους αποστολείς δεν συνεργάζονται όλοι με τον εισβολέα.

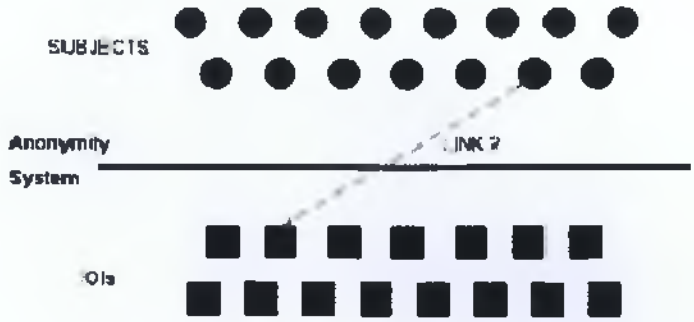
5.3.2. Μετρήσεις ανωνυμίας

Προτού οι πληροφορίες θεωρητικών ανωνυμιών μετρήσεων προταθούν, υπήρξαν κάποιες προσπάθειες να εκτιμηθεί η ανωνυμία στα δίκτυα επικοινωνιών.

Ο Reiter και ο Rubin ορίζουν το βαθμό της ανωνυμίας ως πιθανότητα 1 - p, όπου p είναι η πιθανότητα ανάθεσης από έναν εισβολέα πιθανούς αποστολείς. Σε αυτό το μοντέλο, οι χρήστες είναι πιο ανώνυμοι όπως φαίνονται (προς ένα ορισμένο αντίπαλο) να είναι λιγότερο πιθανό από ότι έστειλε ένα μήνυμα. Αυτή η μέτρηση θεωρεί τους χρήστες ξεχωριστά, και συνεπώς δεν συλλαμβάνει ιδιότητες ανωνυμιών πολύ καλά. Ας θεωρήσουμε αρχικά ένα σύστημα με 2 χρήστες ο οποίος φαίνεται να είναι ο αποστολέας ενός μηνύματος με πιθανότητα 1/2. Τώρα θεωρήστε ένα δεύτερο σύστημα με 1000 χρήστες. Ο χρήστης u1 εμφανίζεται ως ο αποστολέας με πιθανότητα 1/2, ενώ όλοι οι άλλοι χρήστες έχουν ανατεθεί με πιθανότητες αποστολής μηνύματος κάτω από 0.001. Σύμφωνα με τον ορισμό του Reiter και του Rubin, ο βαθμός ανωνυμίας των u1 και των δύο χρηστών του αρχικού συστήματος θα είναι η ίδια (50%). Ωστόσο, στο δεύτερο σύστημα, το u1 φαίνεται πολύ πιο πιθανό να είναι ο αποστολέας από οποιοδήποτε άλλο χρήστη, ενώ οι δύο χρήστες του πρώτου συστήματος είναι πανομοιότυπες στον αντίπαλο.

Ο Bertholdet αϊ. ορίζει το βαθμό ανωνυμίας ως A = log2 (N), όπου N είναι ο αριθμός των χρηστών του συστήματος. Αυτή η μέτρηση εξαρτάται μόνο από τον αριθμό των χρηστών του συστήματος, και επομένως δεν εκφράζουν τις ιδιότητες ανωνυμιών των διαφορετικών συστημάτων. Επιπλέον, οι αντίπαλοι μπορούν να είναι σε θέση να αποκτούν πιθανολογικές πληροφορίες σχετικά με το σύνολο των πιθανών αποστολών, η οποία δεν λαμβάνεται υπόψη σε αυτή την μέτρηση.

Οι πληροφορίες θεωρητικών ανωνυμιών μετρήσεων ήταν ανεξάρτητες προτεινόμενες σε δύο μελέτες που παρουσιάστηκαν στο 2ο Επιστημονικό εργαστήριο Ιδιωτικής Ενίσχυσης Τεχνολογιών. Η βασική αρχή των δύο μετρήσεων είναι η ίδια. Η μέτρησης που προτείνουν ο Serjantov και ο Danezis χρησιμοποιεί εντροπία ως μέτρο της αποτελεσματικής ανωνυμίας καθορισμένου μεγέθους. [5]



Εικόνα 19: Πρότυπο για συστήματα ανωνυμίας

5.4. Μοντέλο

Πολλά συστήματα ανωνυμιών μπορούν να μοντελοποιηθούν από την άποψη της αδυναμίας συνδέσεως. Μη-συνδεσιμότητα ορίζεται από τον Pfitzmann και τον Hansen ως εξής: αδυναμία σύνδεσης δύο ή περισσότερων αντικειμένων σημαίνει ότι μέσα σε αυτό το σύστημα, τα στοιχεία αυτά δεν είναι τίποτα περισσότερο και τίποτα λιγότερο σχετικό από ό, τι σχετίζεται σχετικά με την συμπερασματική γνώση.

Το μοντέλο μπορεί να εφαρμοστεί και στους δυο τον αποστολέα και τον παραλήπτη ανωνυμιών. Αν λάβουμε υπόψη την αποστολή και λήψη των μηνυμάτων, όπως το ItemsofInterest (IOIs), η ανωνυμία μπορεί να οριστεί ως μη-συνδεσιμότητα του IOI και ένας θέματος. Πιο συγκεκριμένα, μπορούμε να περιγράψουμε την ανωνυμία του IOI, όπως ότι δεν συσχετίζονται με οποιοδήποτε θέμα, και η ανωνυμία ενός θέματος δεν συσχετίζεται με οποιαδήποτε IOI. Στο πλαίσιο αυτό, αδυναμίας συνδέσεως επιτυγχάνεται με υψηλή αξία εντροπίας.

Το παραπάνω σχήμα παρουσιάζει ένα απλοποιημένο μοντέλο ανωνυμίας. Ο στόχος των συστημάτων ανωνυμίας είναι να κρύψει τη σχέση μεταξύ των θεμάτων και IOIs. Η απόκρυψη αυτών των συνδέσεων είναι ο βασικός μηχανισμός πίσω από ανώνυμες συναλλαγές.

Ένας παρατηρητής του συστήματος βλέπει ότι ένα σύνολο των χρηστών έχουν πρόσβαση στο σύστημα ανωνυμίας. Κατά την έξοδο του συστήματος, βλέπουν IOIs τα οποία είναι δύσκολα να συνδεθούν με ένα συγκεκριμένο θέμα. Το σύνολο των θεμάτων που μπορεί να συνδεθεί με ένα IOI ονομάζεται σύνολο ανωνυμίας. Μεγαλύτερο σύνολο ανωνυμίας, μεγαλύτερη ανωνυμία απολαμβάνει ένα θέμα. Η έννοια της ανωνυμίας είναι το κλειδί για να ορίσει μετρήσεις ανωνυμίας.[6]

5.5. Μοντέλο επίθεσης

Μπορούμε να διακρίνουμε δύο είδη επιθέσεων κατά των συστημάτων ανωνυμιών: επιθέσεις σχετικά με την ανωνυμία και επιθέσεις σχετικά με τη διαθεσιμότητα της υπηρεσίας ανωνυμίας (επίσης ονομάζεται άρνηση επίθεσης υπηρεσίας). Η άρνηση επίθεσης υπηρεσίας μπορεί να αναπτυχθεί μόνο από ενεργό επιτιθέμενο. Αυτές οι επιθέσεις στοχεύουν στη μείωση της διαθεσιμότητας του συστήματος, η οποία μπορεί να είναι αυτοσκοπός, ή μέρος μιας επίθεσης σχετικά με την ανωνυμία (π.χ., ο αντίπαλος μπορεί να μπλοκάρει διάφορες οντότητες από την πρόσβαση στο σύστημα, για να μειωθεί το σύνολο ανωνυμίας). Στο έγγραφο αυτό, ενδιαφερόμαστε για τις συνέπειες των επιθέσεων ανωνυμίας. Πιο συγκεκριμένα, στη μέτρηση της βεβαιότητας του αντιπάλου για την ύπαρξη συνδέσμου μεταξύ του θέματος και του IOI.

Η ποσοτικοποίηση της ανωνυμίας εξαρτάται από τον εξεταζόμενο αντίπαλο ή εισβολέα. Ο αντίπαλος έχει σίγουρες δυνατότητες και αναπτύσσει επιθέσεις, για να αποκτήσει πληροφορίες και να βρει συνδέσμους μεταξύ των θεμάτων και IOIs. Οι περισσότερες από αυτές τις επιθέσεις οδηγούν σε μια κατανομή πιθανοτήτων που αναθέτουν στους χρήστες μια σίγουρη πιθανότητα να συνδέονται (είτε ως αποστολείς είτε ως παραλήπτες) στο IOIs.

Οι μετρήσεις θα πρέπει να λαμβάνουν υπόψη τις πιθανότητες ανάθεσης από τον αντίπαλο για τους χρήστες που πιθανώς να σχετίζονται με μια IOI. Σημειώνουμε ότι τα μέτρα μέτρησης ανωνυμίας σε σχέση με μια συγκεκριμένη επίθεση τα αποτελέσματα δεν είναι πλέον έγκυρα, εάν το μοντέλο επίθεσης αλλάξει. Συνεπώς, συγκεκριμένες υποθέσεις για τον εισβολέα πρέπει να καθορίζονται ξεκάθαρα κατά τη μέτρηση της ανωνυμίας. Μερικές από τις ιδιότητες του αντιπάλου θα πρέπει να είναι ρητές:

- Παθητικό-Ενεργό (Passive-Active): Ο παθητικός αντίπαλος ακούει την ανακοίνωση ή διαβάζει εσωτερικές πληροφορίες των φορέων που συμμετέχουν στα πρωτόκολλα, οι παθητικοί επιτιθέμενοι συνήθως εκτελούν ανάλυση της κυκλοφορίας της επικοινωνίας. Οι ενεργοί επιτιθέμενοι μπορούν να προσθέσουν, να αφαιρέσουν ή

να τροποποιήσουν τα μηνύματα και να προσαρμόσουν την εσωτερική πληροφόρηση των συμμετεχόντων φορέων.

- Εισερχόμενες-Εξερχόμενες (Internal-External): Μια εσωτερική επίθεση ελέγχει μία ή περισσότερες οντότητες που αποτελούν μέρος του συστήματος (π.χ., ο επιτιθέμενος ελέγχει κόμβους επικοινωνίας). Η εξωτερική επίθεση ελέγχει μόνο τις συνδέσεις επικοινωνίας.
- Μερική-Καθολική (Partial-Global): Μια καθολική επίθεση έχει πρόσβαση σε ολόκληρο το σύστημα επικοινωνίας (π.χ., όλοι οι σύνδεσμοι επικοινωνίας), ενώ η μερική επίθεση (επίσης ονομάζεται τοπικός εισβολέα) βλέπει μόνο ένα μέρος των πόρων (π.χ., ένας περιορισμένος αριθμός των ομότιμων σε ένα peer-to –peer δίκτυο).
- Στάσιμο-Προσαρμοστικό (Static-Adaptive): Η στατική επίθεση ελέγχει ένα προκαθορισμένο σύνολο πόρων και είναι ανίκανο να αλλοιώσει τη συμπεριφορά τους, όταν μια συναλλαγή είναι σε εξέλιξη. Η προσαρμοσμένη επίθεση αποκτάει τον έλεγχο σε νέους πόρους ή τροποποιεί τη συμπεριφορά τους, βασιζόμενο στα ενδιάμεσα αποτελέσματα της επίθεσης.
- Προσωρινό-Μόνιμο (Temporary-Permanent): Ο μόνιμος αντίπαλος έχει παρατηρήσει το σύστημα καθώς ξεκίνησε να λειτουργεί και ξέρει όλη την ιστορία. Η προσωρινή επίθεση άρχισε να παρατηρεί ή να επιτίθεται στο σύστημα τη χρονική στιγμή t0, και δεν έχουν πληροφορίες σχετικά με τα γεγονότα πριν από την t0.[5]

5.6. Πληροφορίες θεωρητικών ανωνυμιών μετρήσεων

Σε αυτό το σημείο θα παρουσιάσουμε την έννοια της εντροπίας, στην οποία βασίζονται οι πληροφορίες θεωρητικών ανωνυμιών μετρήσεων. Στη συνέχεια, θα εξηγήσουμε πως το αποτελεσματικό μέγεθος ανωνυμίας και ο βαθμός ανωνυμίας μπορεί να υπολογιστεί.

Εντροπία

Η έννοια της θεωρίας πληροφοριών της εντροπίας παρέχει ένα μέτρο της αβεβαιότητας μιας τυχαίας μεταβλητής. Έστω X η διακριτή τυχαία μεταβλητή με πιθανότητα λειτουργία μαζικής pi = Pr (X = i), όπου i αντιπροσωπεύει κάθε πιθανή τιμή X που μπορεί να λάβει με πιθανότητα pi> 0. Στην περίπτωση αυτή, κάθε i αντιστοιχεί σε ένα θέμα σετ ανωνυμίας, δηλαδή, Pi είναι η πιθανότητα αντικειμένου i που συνδέεται με την IOI. Συμβολίζουμε με H (X) την εντροπία μιας τυχαίας

μεταβλητής, και n ο αριθμός των θεμάτων στο σύνολο της ανωνυμίας. H (X) μπορεί να υπολογιστεί ως:

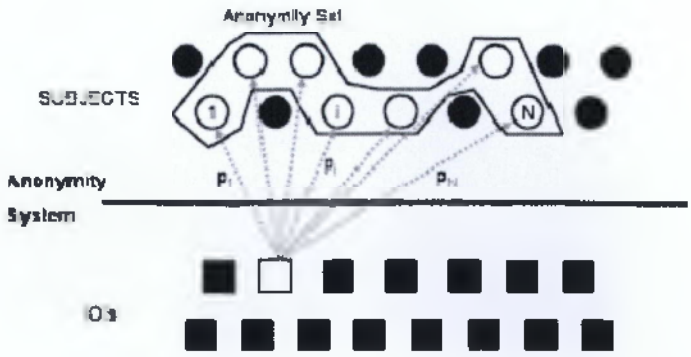
$$H(X) = -\sum_{i=1}^{N} p_i \log_2(p_i)$$

Αποτελεσματικό μέγεθος ανωνυμίας

Το αποτελεσματικό μέγεθος του σετ ανωνυμίας είναι ένα ενδιάμεσο βήμα για να υπολογιστεί ο βαθμό της ανωνυμίας. Ο Serjantov και ο Danezis πρότειναν τη χρήση του πραγματικού μεγέθους σετ ανωνυμία ως μετρική.

Η ανωνυμία ορίστηκε από τον Pfitzmann και τον Hansen ως η κατάσταση του να μην είναι αναγνωρίσιμα μέσα σε ένα σύνολο θεμάτων, το σύνολο της ανωνυμίας. Οι Μετρήσεις ανωνυμίας αποσκοπούν στο να δώσουν ένα ουσιαστικό μέτρο για το συνολικό μέγεθος της ανωνυμίας.

Μετά την ανάπτυξη μια επίθεσης σε ένα σύστημα ανωνυμίας, ο αντίπαλος συνήθως αποκτά μια κατανομή πιθανοτήτων τα θέματα που συνδέονται με τη συγκεκριμένη IOI επίθεσης. Οι πιθανότητες φαίνεται στο σχήμα. 20 με τα βέλη που συνδέουν τα IOI στα θέματα του συνόλου ανωνυμίας. Διαφορετικά θέματα μπορεί να εμφανιστούν ως υψηλότερη ή χαμηλότερη pi πιθανότητα σύνδεσης με το IOI, εξαρτώμενο με τις πληροφορίες που απέκτησε από την αντίπαλη επίθεση.



Εικόνα 20: Τοποθέτηση ανωνυμιών

Ας υποθέσουμε N είναι ο συνολικός αριθμός των θεμάτων που συνδέονται με την ΙΟΙ με μη μηδενική πιθανότητα (pi> 0, i = 1 .. N). Το πραγματικό μέγεθος του σετ ανωνυμία ορίζεται ως η εντροπία H (X) της κατανομής X πιθανοτήτων που συνδέουν τα θέματα της ανωνυμίας στο ΙΟΙ.

Η εντροπία βασίζεται σε μετρικές ανωνυμίας που δίνουν ένα μέτρο της αβεβαιότητας του αντιπάλου σχετικά με το θέμα που σχετίζεται με το ΙΟΙ. Το πραγματικό μέγεθος του σετ ανωνυμίας λαμβάνει υπόψη τον αριθμό των πιθανών θεμάτων που συνδέονται με την ΙΟΙ, και οι πιθανότητες εκχωρούνται στα επιμέρους θέματα.

Οι μετρήσεις (και συνεπώς ανωνυμίας) αυξάνει την αξία των δύο παραγόντων. Πρώτον, με τον αριθμό των θεμάτων που συνδέεται συνήθως με το ΙΟΙ, και το δεύτερο, με την ομοιομορφία της κατανομής πιθανοτήτων. Η ποιο ισομερής κατανομή πιθανοτήτων αναθέτει στα θέματα του συνόλου ανωνυμίας, υψηλότερηεντροπία.

Βαθμός ανωνυμίας

Ο βαθμός της ανωνυμίας είναι μια ομαλοποιημένη έκδοση του πραγματικού μεγέθους σετ ανωνυμίας, η οποία λέει πόσο καλό είναι το σύστημα που αποδίδει σε μια κλίμακα 0-1. Αυτή η μέτρηση είναι μια πρωτότυπη συμβολή των D'IAZ etal. και η οποία προτάθηκε.

Το μέγιστο αποτελεσματικό μέγεθος ανωνυμία για N θέματα επιτυγχάνεται όταν όλα τα θέματα που συνδέονται με την ΙΟΙ έχουν ισομερή πιθανότητα (δηλαδή, pi = 1 / N). Σε αυτή την περίπτωση, όλα τα θέματα είναι πανομοιότυπα προς τον αντίπαλο σε σχέση με το ΙΟΙ. Για ένα δεδομένο N αριθμός χρηστών, η μέγιστη επιτεύξιμη ανωνυμίας αντιστοιχεί στην εντροπία της ομοιόμορφης κατανομής. Ορίζουμε τη μέγιστη εντροπία ως HM:

$$H_M = \log_2(N)$$

Αν υποθέσουμε ότι ο αντίπαλος δεν έχει συμπερασματική πληροφορία σχετικά με το σύστημα (δηλαδή, η συμπερασματική ανωνυμία του ΙΟΙ είναι HM), η ποσότητα των πληροφοριών που έχουν αποκτηθεί από τον αντίπαλο με μια επίθεση είναι η διαφορά στην εντροπία πριν και μετά την επίθεση, αυτό είναι: HM - H (X). Ο βαθμός της

ανωνυμίας ορίζεται ως η ομαλοποιημένη τιμή αυτής της διαφοράς στις γνώσεις του αντιπάλου:

$$d = 1 - \frac{H_M - H(X)}{H_M} = \frac{H(X)}{H_M}$$

Όπως μπορούμε να παρατηρήσουμε στον τύπο, ο βαθμός της ανωνυμίας λαμβάνεται διαιρώντας το αποτελεσματικό μέγεθος σετ ανωνυμία από τη μέγιστη εντροπία για ένα δεδομένο αριθμό θεμάτων. Αυτός ο βαθμός αξιολογεί πόση ανωνυμία παρέχεται από ένα σύστημα ανεξάρτητα από τον αριθμό των χρηστών. Λαμβάνοντας υπόψη ένα ορισμένο αριθμό των θεμάτων, ο υπολογισμός του βαθμού ανωνυμίας δίνει μια ιδέα για το πόσο η ανωνυμία των θεμάτων είναι κοντά στο μέγιστο εφικτό.

Και οι δύο μετρήσεις υπολογίζονται χρησιμοποιώντας τις ίδιες πληροφορίες, και μπορεί κανείς να υπολογιστεί επιπόλαια από το άλλο. Η διαφορά είναι, ωστόσο, ότι το αποτελεσματικό μέγεθος σετ ανωνυμίας δένει την ανωνυμία με τον πραγματικό αριθμό των χρηστών στο σύστημα, ενώ ο βαθμός της ανωνυμίας κάνει αφαίρεση από τον αριθμό των χρηστών και επικεντρώνεται στις επιδόσεις του συστήματος.[6]

Βιβλιογραφία

Δημοσιεύσεις

[1] Kanubhai K. Patel- Bharat V. Buddhader, «An Architecture of Hybrid Intrusion Detection System»

[2] Nenod Dulanovic- Dane Hinic- Dejan Simic, «An Intrusion Prevention System as a Proactive Security Mechanism in Network Infrastructure»

[3] Amin Rasoulifard- Abbas Ghaemi Bafghi- Monsen Kahani, « Incremental Hybrid Intrusion Detection Using Ensemble for Weak Classifiers

[4] R. Rangadurai Karthick- Vipul P. Hattiwale- Balaraman Ravindran, «Adaptive Network Intrusion Detection System Using a Hybrid Approach

[5] Claudia Diaz, «Anonymity Metrics Revisited»

[6] Dogan Kesdogan- Lexi Pimenidis, «The Hitting Attack on Anonymity Protocols»

[7] Elsam Mohsin Hossib- Aida Osma Abdelgwed- Ahmed Ibrahim Saleh, « A Hybrid Intrsuion Prevention System for Web Database Security»

[8] Αδάμου Αλεξάνδρου, «Σχεδίαση και ανάπτυξη μηχανισμού για τη δυναμική ανίχνευση αργών επιθέσεων σε συστήματα ανίχνευσης εισβολής»

[9] Παλαντάς Παναγιώτης, «Μελέτη, σχεδιασμός και ενσωμάτωση συστήματος ανίχνευσης δικτυακών επιθέσεων σε εργαστηριακό περιβάλλον»

[10] Δημόπουλος Βασίλης, «Αξιολόγηση Λογισμικού Ανίχνευσης Δικτυακών Εισβολών με Υποβοήθηση από Υλικό», Πολυτεχνείο Κρήτης

[11] Vern Paxson, «Bro: A system for Detecting Network Intruders in Real-Time»

[12] Robin Sommer, «Bro: An Open Source Network Intrusion Detection System»

[13] Pritika Mehra, «A brief stydy and comparison of Snort and Bro Open Source Network Intrusion Detection System»

[14] Shaffai Gupta-Rahit Goel, «A Graphical User Interface Framework for Detecting Intrusion using Bro IDS»

[15] Κουρκοβέλης Ανδρέας, «Διδακτική της Τεχνολογίας και Ψηφιακά Συστήματα»

Τεχνικές Αναφορές

[16] Οικονόμου Ευθύμιος, « Μελέτη και ανάλυση των συστημάτων ανίχνευσης εισβολών», Πανεπιστήμιο Πειραιώς

[17] Divya- Surender Lakra, «H- Snort: A Hybrid Intrusion Detection System Using Artificial Intelligence with Snort

[18] Δρ. Σ. Βελούδη, «Βασικές Έννοιες»

[19] Zhneqi Wang- Dankai Zhang, «HIDS and NIDS Intrusion Detection System Model Design»

[20] Jack Timofte, «Intrusion Detection using Open Source Tools»

[21] J. Gomez- C. Gil- N. Padilla- R. Banos- C. Jimenez, « Design of a Snort-Based Hybrid Intrusion Detection System»

[22] Λιούτας Θανάσης-Πάτσιας Μιχαήλ, «Μετά-επεξεργασία συναργεμών IDS Συστημάτων»

[23] Asmaa Shaker Ashoor, «Intrusion Detection System & Intrusion prevention System»

Βιβλία

[24] Μπάρδης Γ. -Νικολόπουλος Β.-Μπράττος Ι. «Μελέτες- Εφαρμογές & Υλοποίηση Δικτύων Η/Υ»

[25] Steve Piper, «Intrusion Prevention System»

Ιστοσελίδες

[26] http://en.wikipedia.org/wiki/Intrusion_prevention_system#Classifications

[27] http://en.wikipedia.org/wiki/Snort_(software)

[28] http://en.wikipedia.org/wiki/Bro_(software)

[29] http://www.sans.org/reading-room/whitepapers/detection/web-application-attack-analysis-bro-ids-34042

[30] http://www.sans.org/reading-room/whitepapers/detection/web-application-attack-analysis-bro-ids-34042

[31] http://www.webopedia.com/DidYouKnow/Computer_Science/2005/intrusion_detection_prevention.asp

[32] https://corisweb.stsisp.ro/tools/ips_ids#sec232

[33] http://ubiquity.acm.org/article.cfm?id=1071927

[34] http://www.safensoft.com/hips/

[35] http://www.jawconsulting.co.uk/technologies/network-intrusion-prevention-systems

[36] http://www.sans.org/reading-room/whitepapers/detection/network-ids-ips-deployment-strategies-2143?show=network-ids-ips-deployment-strategies-2143&cat=detection

[37] http://itlaw.wikia.com/wiki/Network-based_intrusion_prevention_system

[38] https://www.ibm.com/developerworks/library/se-intrusion/

[39] http://en.wikipedia.org/wiki/OSSEC

[40] http://ktaraghi.blogspot.gr/2013/02/ossec-host-based-intrusion-detection-in.html

[41] http://www.chrisbrenton.org/2010/02/combining-logwatch-and-ossec-%E2%80%93-part-2/

[42] http://www.clshack.it/nopaste/ossec_tutorial/CSC570E_Research_Paper_OSSEC.pdf

[43] http://www.giac.org/paper/gcih/7549/practical-ossec/115906

[44] http://en.wikipedia.org/wiki/Suricata_(software)

[45] http://suricata-ids.org/

[46] https://home.regit.org/2012/02/ecosystem-of-suricata/

[47] http://www.authorstream.com/Presentation/kittukind-908740-intrusion-prevention-system/

[48] http://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%91%CE%BD%CE%AF%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82_%CE%95%CE%B9%CF%83%CE%B2%CE%BF%CE%BB%CE%AE%CF%82

[49] http://greg61.gr/blog/%CE%B7-%CE%B3%CF%89%CE%BD%CE%B9%CE%AC-%CF%84%CE%BF%CF%85-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE-%CE%BA%CE%B1%CE%B9-%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84/%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD-%CE%BA%CE%B1%CE%B9-%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD/%CE%BA%CE%B5%CF%86%CE%AC%CE%BB%CE%B1%CE%B9%CE%BF-4-

%CF%87%CE%B5%CE%B9%CF%81%CE%B9%CF%83%CE%BC%CE%BF%CE%AF-
%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%AF%CE%B1%CF%82-
%CF%83%CF%84%CE%B1-%CE%B4/

[50] http://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%
B7%CE%BC%CE%B1 %CE%91%CE%BD%CE%AF%CF%87%CE%BD%CE%B5%CF%85%CF%83
%CE%B7%CF%82 %CE%95%CE%B9%CF%83%CE%B2%CE%BF%CE%BB%CE%AE%CF%82