Συστήματα ανίχνευσης εισβολής Snort

Principles of Cybersecurity

Αντρέας Προδρόμου

Τα συστήματα ανίχνευσης εισβολής δικτύου NIDS αποτελούν σημαντικό μέρος οποιασδήποτε αρχιτεκτονικής ασφάλειας δικτύου. Παρέχουν ένα επίπεδο άμυνας που παρακολουθεί την κυκλοφορία του δικτύου για προκαθορισμένη ύποπτη δραστηριότητα ή μοτίβα και ειδοποιεί τους διαχειριστές του συστήματος όταν εντοπίζεται πιθανή εχθρική κίνηση. Τα εμπορικά IDS έχουν πολλές διαφορές, αλλά τα τμήματα πληροφοριακών συστημάτων πρέπει να αντιμετωπίσουν τα κοινά σημεία που μοιράζονται, όπως αποτύπωμα συστήματος, περίπλοκη ανάπτυξη και υψηλό χρηματικό κόστος. Το Snort σχεδιάστηκε για να αντιμετωπίσει αυτά τα ζητήματα.

Η ανίχνευση εισβολής είναι ένα σύνολο τεχνικών και μεθόδων που χρησιμοποιούνται για τον εντοπισμό ύποπτης δραστηριότητας τόσο σε επίπεδο δικτύου όσο και σε επίπεδο κεντρικού υπολογιστή. Τα συστήματα ανίχνευσης εισβολής εμπίπτουν σε δύο βασικές κατηγορίες σε συστήματα ανίχνευσης εισβολής που βασίζονται σε υπογραφές και σε συστήματα ανίχνευσης ανωμαλιών. Για παράδειγμα οι εισβολείς έχουν υπογραφές οπου μπορούν να εντοπιστούν χρησιμοποιώντας το λογισμικό. Επίσης προσπαθεί να βρει πακέτα δεδομένων που περιέχουν οποιαδήποτε σχετίζεται με εισβολή ή ανωμαλίες που σχετίζονται με πρωτόκολλα Διαδικτύου. Βασισμένο σε ένα σύνολο υπογραφών και κανόνες, το σύστημα ανίχνευσης είναι σε θέση να βρει και να καταγράψει ύποπτη δραστηριότητα και να δημιουργήσει ειδοποιήσεις. Η ανίχνευση εισβολής που βασίζεται σε ανωμαλίες εξαρτάται συνήθως από ανωμαλίες πακέτων υπάρχουν σε μέρη της κεφαλίδας πρωτοκόλλου. Σε ορισμένες περιπτώσεις αυτές οι μέθοδοι παράγουν καλύτερα

αποτελέσματα σε σύγκριση με τα IDS που βασίζονται στην υπογραφή. Συνήθως ένα σύστημα ανίχνευσης εισβολής καταγράφει δεδομένα από το δίκτυο και εφαρμόζει τους κανόνες του σε αυτά τα δεδομένα ή εντοπίζει ανωμαλίες σε αυτά. Το Snort είναι κυρίως ένα IDS που βασίζεται σε κανόνες, ωστόσο υπάρχουν plugs εισόδου για ανίχνευση ανωμαλίων στις κεφαλίδες του πρωτοκόλλου.

Το Snort είναι ένα σύστημα πρόληψης εισβολής δικτύου NIPS και σύστημα εντοπισμού εισβολής δικτύου NIDS που είναι δωρεάν και ανοιχτού κώδικα. Επίσης το Snort γεμίζει μια σημαντική θέση στη σφαίρα της ασφάλειας του δικτύου. Είναι ένα ελαφρύ εργαλείο ανίχνευσης εισβολών δικτύου πολλαπλών πλατφορμών που μπορεί να αναπτυχθεί για την παρακολούθηση μικρών δικτύων TCP/IP και τον εντοπισμό μεγάλης ποικιλίας ύποπτης κίνησης δικτύου καθώς και απροκάλυπτων επιθέσεων. Μπορεί να παρέχει στους διαχειριστές αρκετά δεδομένα για τη λήψη τεκμηριωμένων αποφάσεων σχετικά με τη σωστή πορεία δράσης σε περίπτωση ύποπτης δραστηριότητας. Το Snort μπορεί επίσης να αναπτυχθεί γρήγορα για να γεμίσει πιθανές τρύπες στην κάλυψη ασφαλείας ενός δικτύου, όταν εμφανίζεται νέα επίθεση. Το Snort είναι ένα εργαλείο για μικρά και ελαφρώς χρησιμοποιούμενα δίκτυα. Το Snort είναι χρήσιμο όταν δεν είναι οικονομικά αποδοτική η ανάπτυξη εμπορικών αισθητήρων NIDS. Τα σύγχρονα εμπορικά συστήματα ανίχνευσης εισβολών κοστίζουν χιλιάδες δολάρια τουλάχιστον, δεκάδες ή και εκατοντάδες χιλιάδες σε ακραίες περιπτώσεις. Ο Marty Roesch το σχεδίασε το 1998, το Snort διατίθεται υπό την General Public License και είναι δωρεάν για χρήση σε οποιοδήποτε περιβάλλον, καθιστώντας την χρήση του Snort ως ένα σύστημα ασφάλειας δικτύου περισσότερο σε θέματα διαχείρισης και συντονισμού δικτύου.

Το Snort είναι κατάλληλο για να καλύψει τους ρόλους της ασφάλειας του δικτύου. Στις περισσότερες σύγχρονες αρχιτεκτονικές το Snort παίρνει λίγα μόνο λεπτά για να συνταχθεί και να τεθεί σε εφαρμογή, και ίσως άλλα δέκα λεπτά για ρύθμιση και ενεργοποίηση. Συγκρίνετε με πολλά εμπορικά IDS, τα οποία απαιτούν αποκλειστικές πλατφόρμες και εκπαίδευση χρηστών για την ανάπτυξη με ουσιαστικό τρόπο. Το Snort μπορεί να διαμορφωθεί και να λειτουργεί για μεγάλα χρονικά διαστήματα χωρίς να απαιτείται παρακολούθηση ή διοικητική συντήρηση, και μπορεί ακόμη να χρησιμοποιηθεί και ως αναπόσπαστο μέρος των περισσότερων υποδομών ασφάλειας δικτύου. Το Snort είναι ένας ανιχνευτής πακέτων που βασίζεται σε libpcap και καταγραφικό που

μπορεί να χρησιμοποιηθεί ως ένα ελαφρύ δίκτυο σύστημα ανίχνευσης εισβολής δηλαδή IDS. Διαθέτει καταγραφή βάσει κανόνων για την εκτέλεση αντιστοίχισης μοτίβων περιεχομένου και τον εντοπισμό μιας ποικιλίας επιθέσεων και ανιχνευτών, όπως stealth port scans, επιθέσεις CGI, buffer overflows, και πολλά άλλα. Το Snort έχει σε πραγματικό χρόνο δυνατότητα ειδοποίησης, με ειδοποιήσεις που αποστέλλονται στο syslog και στο μπλοκ μηνυμάτων διακομιστή ή ένα ξεχωριστό αρχείο ειδοποίησης. Το Snort ρυθμίζεται χρησιμοποιώντας διακόπτες γραμμής εντολών και προαιρετικό πακέτο φιλτράρισμα εντολών. Η μηχανή ανίχνευσης είναι προγραμματίζεται χρησιμοποιώντας μια απλή γλώσσα που περιγράφει δοκιμές και ενέργειες ανά πακέτο. Η ευκολία χρήσης απλοποιεί και επιταχύνει την ανάπτυξη νέων κανόνων ανίχνευσης εκμετάλλευσης. Επίσης το Snort είναι ευκολότερο οικονομικά, τεχνικά σαν εφαρμογή από άλλα εργαλεία ανοιχτού κώδικα ή εμπορικά διαθέσιμα.

Το κύριο χαρακτηριστικό που έχει το Snort είναι ότι αποκωδικοποιεί το επίπεδο εφαρμογής ενός πακέτου και μπορεί να του δοθούν κανόνες για τη συλλογή επισκεψιμότητας που περιέχει συγκεκριμένα δεδομένα στο επίπεδο εφαρμογής του. Αυτό επιτρέπει στο Snort να ανιχνεύει πολλούς τύπους εχθρικής δραστηριότητας, αδυναμίες των CGI ή οποιωνδήποτε άλλων δεδομένων στο ωφέλιμο φορτίο πακέτων που μπορούν να χαρακτηριστούν ένα μοναδικό δακτυλικό αποτύπωμα ανίχνευσης. Ένα άλλο πλεονέκτημα του Snort είναι ότι η αποκωδικοποιημένη οθόνη εξόδου του είναι κάπως πιο φιλική προς το χρήστη. Το Snort δεν αναζητά ονόματα κεντρικών υπολογιστών ή ονόματα θυρών κατά την εκτέλεση αλλά εστιάζει στη συλλογή πακέτων όσο το δυνατόν γρηγορότερα και στην επεξεργασία τους στη μηχανή ανίχνευσης Snort. Η εκτέλεση αναζήτησης ονόματος κεντρικού υπολογιστή σε χρόνο εκτέλεσης δεν ευνοεί την ανάλυση πακέτων υψηλής απόδοσης. Ένα ισχυρό χαρακτηριστικό του Snort, είναι η δυνατότητα φιλτραρίσματος της κυκλοφορίας με εντολές Berkeley Packet Filter(BPF). Επίσης το Snort μπορεί να χρησιμοποιήσει τους ευέλικτους κανόνες του για να εκτελέσει πρόσθετες λειτουργίες, όπως η αναζήτηση και η καταγραφή μόνο εκείνων των πακέτων που έχουν οριστεί με συγκεκριμένο τρόπο τις σημαίες TCP τους ή που περιέχουν αιτήματα ιστού που ισοδυναμούν με ανιχνευτές ευπάθειας CGI. Οι ανιχνευτές πακέτων και οι επιθέσεις μπορούν να καταγραφούν και οι ειδοποιήσεις μπορούν αποστέλλονται αυτόματα από το Snort.

Η αρχιτεκτονική του Snort επικεντρώνεται στην απόδοση, απλότητα και ευελιξία. Υπάρχουν τρία κύρια υποσυστήματα που απαρτίζουν το Snort, ο αποκωδικοποιητής πακέτων, η μηχανή ανίχνευσης και το υποσύστημα καταγραφής και ειδοποίησης. Αυτά τα υποσυστήματα οδηγούν το libpcap, βιβλιοθήκη sniffing πακέτων, η οποία παρέχει φορητή δυνατότητα ανίχνευσης και φιλτραρίσματος πακέτων, διαμόρφωση του προγράμματος, ανάλυση κανόνων και δομή δεδομένων. Η καταγραφή πραγματοποιείται πριν από την προετοιμασία του τμήματος sniffer, διατηρώντας το ποσό της επεξεργασίας ανά πακέτο στο ελάχιστο που απαιτείται για την επίτευξη του βασικού προγράμματος λειτουργικότητα.

Το Snort χωρίζεται σε μερικά στοιχεία, μέρη. Αυτά τα στοιχεία συνεργάζονται για να εντοπίσουν συγκεκριμένες επιθέσεις και να παράγουν αποτελέσματα με τη μορφή που απαιτεί το σύστημα ανίχνευσης. Τα ακόλουθα είναι τα κύρια στοιχεία ενός IDS που βασίζεται το Snort και είναι η αποκωδικοποιητής πακέτων(packet decoder), οι προεπεξεργαστές(preprocessors), η μηχανή ανίχνευσης(detection engine), το σύστημα καταγραφής και ειδοποίησης(logging and alerting) , μονάδες εξόδου.

Το Snort λειτουργεί σαν packet decoder όπου είναι οργανωμένο γύρω από τα στρώματα της στοίβας πρωτοκόλλου που υπάρχει στον υποστηριζόμενο σύνδεσμο δεδομένων και στους ορισμούς πρωτοκόλλου TCP/IP. Ο packet decoder επιβάλλει την τάξη στα δεδομένα πακέτων επικαλύπτοντας δομές δεδομένων στην ακατέργαστη κίνηση του δικτύου. Οι υποεργασίες αποκωδικοποίησης καλούνται με τη σειρά μέσω της στοίβας πρωτοκόλλου, από το επίπεδο ζεύξης δεδομένων προς τα πάνω μέσω του επιπέδου μεταφοράς, καταλήγοντας τελικά στο επίπεδο εφαρμογής. Η ταχύτητα τονίζεται σε αυτήν την ενότητα και η πλειοψηφία της λειτουργικότητας του αποκωδικοποιητή συνίσταται στη ρύθμιση δεικτών στα δεδομένα του πακέτου για μεταγενέστερη ανάλυση από τη μηχανή ανίχνευσης. Το Snort παρέχει δυνατότητες αποκωδικοποίησης για πρωτόκολλα σύνδεσης δεδομένων ethernet. Επίσης αντί να εμφανίζει τα πακέτα που διαβάζει από το δίκτυο στην οθόνη, η εφαρμογή τα καταγράφει στο δίσκο σε λειτουργία καταγραφής πακέτων έτσι όταν απαιτείται μελέτη των πακέτων που διαβάζονται, αυτή η δυνατότητα είναι χρήσιμη. Το Snort μπορεί να αποθηκεύσει πακέτα σε διάφορες μορφές, συμπεριλαμβανομένης της δυαδικής μορφής (tcpdump), η οποία μπορεί να χρησιμοποιηθεί ως είσοδος σε μια σειρά άλλων προγραμμάτων που αναλύουν πακέτα και πρωτόκολλα. Η

λειτουργία αυτή συνήθως λειτουργεί παράλληλα από τις λειτουργίες sniffer ή NIDS . Ο αποκωδικοποιητής πακέτων λαμβάνει πακέτα από διαφορετικούς τύπους διεπαφών δικτύου και προετοιμάζει τα πακέτα για προεπεξεργασία ή αποστολή στη μηχανή ανίχνευσης. Οι διεπαφές μπορεί να είναι Ethernet, SLIP, PPP και ούτω καθεξής.

Οι προεπεξεργαστές είναι στοιχεία ή πρόσθετα που μπορούν να χρησιμοποιηθούν με το Snort για να τακτοποιήσουν ή να τροποποιήσουν πακέτα δεδομένων προτού η μηχανή ανίχνευσης κάνει κάποια ενέργεια για να διαπιστώσει εάν το πακέτο χρησιμοποιείται από εισβολέα. Ορισμένοι προεπεξεργαστές εκτελούν επίσης ανίχνευση βρίσκοντας ανωμαλίες στις κεφαλίδες πακέτων και δημιουργώντας ειδοποιήσεις. Οι προεπεξεργαστές είναι πολύ σημαντικοί για κάθε IDS να προετοιμάσει πακέτα δεδομένων που θα αναλυθούν με βάση τους κανόνες στη μηχανή ανίχνευσης. Οι χάκερς χρησιμοποιούν διαφορετικές τεχνικές για να ξεγελάσουν ένα IDS με διαφορετικούς τρόπους. Για παράδειγμα, μπορεί να έχετε δημιουργήσει έναν κανόνα για να βρείτε μια υπογραφή scripts/iisadmin σε πακέτα HTTP. Εάν ταιριάζετε ακριβώς αυτή τη συμβολοσειρά, μπορείτε εύκολα να ξεγελαστείτε από έναν χάκερ που κάνει μικρές τροποποιήσεις σε αυτήν τη συμβολοσειρά. Ένας προεπεξεργαστής μπορεί να αναδιατάξει τη συμβολοσειρά έτσι ώστε να είναι ανιχνεύσιμη από το IDS. Οι προεπεξεργαστές χρησιμοποιούνται επίσης για την ανασυγκρότηση πακέτων. Όταν ένα μεγάλο κομμάτι δεδομένων μεταφέρεται σε έναν κεντρικό υπολογιστή, το πακέτο είναι συνήθως κατακερματισμένο. Οι χάκερς χρησιμοποιούν κατακερματισμό για να νικήσουν τα συστήματα ανίχνευσης εισβολής. Οι προεπεξεργαστές χρησιμοποιούνται για την προστασία από αυτές τις επιθέσεις. Οι προεπεξεργαστές στο Snort μπορούν να ανασυγκροτήσουν πακέτα, να αποκωδικοποιήσουν HTTP URI, να συναρμολογήσουν ροές TCP, UDP και αλλά πρωτοκολλά. Αυτές οι λειτουργίες αποτελούν πολύ σημαντικό μέρος του συστήματος ανίχνευσης εισβολής.

Η μηχανή ανίχνευσης detection engine είναι το πιο σημαντικό μέρος του Snort. Η ευθύνη του είναι να ανιχνεύσει εάν υπάρχει δραστηριότητα εισβολής σε ένα πακέτο. Η μηχανή ανίχνευσης χρησιμοποιεί κανόνες Snort για αυτό το σκοπό. Οι κανόνες διαβάζονται σε εσωτερικές δομές δεδομένων ή αλυσίδες όπου ταιριάζουν με όλα τα πακέτα. Εάν ένα πακέτο ταιριάζει με οποιονδήποτε κανόνα, λαμβάνονται τα κατάλληλα μέτρα. διαφορετικά το πακέτο απορρίπτεται. Οι κατάλληλες ενέργειες μπορεί να είναι η καταγραφή του πακέτου ή η δημιουργία ειδοποιήσεων. Η μηχανή ανίχνευσης είναι το κρίσιμο για τον

χρόνο μέρος του Snort. Ανάλογα με το πόσο ισχυρό είναι το μηχάνημά σας και πόσους κανόνες έχετε ορίσει, μπορεί να χρειαστεί διαφορετικός χρόνος για να ανταποκριθεί σε διαφορετικά πακέτα. Εάν η επισκεψιμότητας στο δίκτυό σας είναι πολύ υψηλή όταν το Snort λειτουργεί σε λειτουργία NIDS, ενδέχεται να απορρίψετε ορισμένα πακέτα και ενδέχεται να μην λάβετε πραγματική απόκριση σε πραγματικό χρόνο. Επίσης διατηρεί τους κανόνες ανίχνευσης σε δύο διαστάσεων συνδεδεμένη λίστα με αυτά που ονομάζονται chain headers και chain options. Αυτοί είναι κατάλογοι κανόνων που έχουν συμπυκνωθεί σε μια λίστα κοινών χαρακτηριστικά στις chain headers, με την ανίχνευση και την επιλογή τροποποίησης που περιέχονται στις chain options. Για παράδειγμα, οι κανόνες ανίχνευσης καθορίζονται σε ένα δεδομένο αρχείο βιβλιοθήκης ανίχνευσης snort και μοιράζονται κοινές διευθύνσεις IP προέλευσης και προορισμού και θύρες. Για να επιταχύνετε την ανίχνευση και επεξεργασία, αυτά τα κοινά στοιχεία συμπυκνώνονται. Αυτές οι αλυσίδες κανόνων αναζητούν αναδρομικά για κάθε πακέτο και προς τις δύο κατευθύνσεις. Η μηχανή ανίχνευσης ελέγχει τις chain options που έχουν οριστεί από τον αναλυτή κανόνων κατά το χρόνο εκτέλεσης. Ο μηχανισμός ανίχνευσης εισβολής του Snort βασίζεται κυρίως στη μέθοδο κακής χρήσης με τη χρήση κακόβουλων πακέτων. Ωστόσο, το Snort έχει συνδυάσει στην ανάλυση λειτουργίας των γεγονότων για τον εντοπισμό πιθανών επιθέσεων με ορισμένες από τις μεθόδους του πρωτοκόλλου ανίχνευσης διαταραχών δηλαδή ανίχνευση ανωμαλίας πρωτοκόλλου και της ακατάλληλης συμπεριφοράς πρωτοκόλλου δηλαδή ανίχνευση κακής χρήσης. Αυτές οι τεχνικές επιτυγχάνονται μέσω προ επεξεργαστών, αλλά και από το νέο του σύστημα το οποίο οργανώνει τους κανόνες σε κατηγορίες.

Στη λειτουργία sniffer, η εφαρμογή διαβάζει πακέτα δικτύου και τα δείχνει στον χρήστη με ωραίο στυλ στην οθόνη, κάνοντας ουσιαστικά μια εγγραφή κίνησης δικτύου. Είναι δυνατό να επιλέξετε τον τύπο των πακέτων που θα εμφανίζονται για το πρωτόκολλο, τον αποστολέα, τον παραλήπτη και πολλές άλλες ιδιότητες ενός πακέτου χρησιμοποιώντας διάφορα που μπορεί να χρησιμοποιήσει ο χρήστης. Εάν ένας χρήστης πληκτρολογήσει τη λέξη κλειδί, θα εμφανίζονται μόνο τα πακέτα που υλοποιούν αυτό το πρωτόκολλο.

Επίσης το υποσύστημα ειδοποίησης και καταγραφής δηλαδή το alerting and logging επιλέγεται στον χρόνο εκτέλεσης με διακόπτες γραμμής εντολών. Αυτήν τη στιγμή υπάρχουν τρεις επιλογές καταγραφής και πέντε επιλογές ειδοποίησης. Οι επιλογές καταγραφής

μπορούν να ρυθμιστούν ώστε να καταγράφουν πακέτα στην αποκωδικοποίησή τους και η μορφή τους είναι αναγνώσιμη από τον άνθρωπο σε μια δομή καταλόγου που βασίζεται σε IP ή σε δυαδική μορφή σε ένα μεμονωμένο αρχείο καταγραφής. Η καταγραφή αποκωδικοποιημένης μορφής επιτρέπει γρήγορη ανάλυση δεδομένα που συλλέγονται από το σύστημα. Η μορφή tcpdump είναι πολύ πιο γρήγορα για εγγραφή στο δίσκο και θα πρέπει να χρησιμοποιείται σε περιπτώσεις όπου απαιτείται υψηλή απόδοση. Η καταγραφή μπορεί επίσης να απενεργοποιηθεί εντελώς, αφήνοντας ειδοποιήσεις ενεργοποιημένη για ακόμη μεγαλύτερες βελτιώσεις απόδοσης. Ανάλογα με το τι βρίσκει η μηχανή ανίχνευσης μέσα σε ένα πακέτο, το πακέτο μπορεί να χρησιμοποιηθεί για την καταγραφή της δραστηριότητας ή τη δημιουργία ειδοποίησης. Τα αρχεία καταγραφής διατηρούνται σε απλά αρχεία κειμένου, αρχεία τύπου tcpdump ή κάποια άλλη μορφή. Όλα τα αρχεία καταγραφής αποθηκεύονται στον φάκελο snort από προεπιλογή. Μπορείτε να χρησιμοποιήσετε τις επιλογές της γραμμής εντολών για να τροποποιήσετε τη θέση δημιουργίας αρχείων καταγραφής και ειδοποιήσεων.

Οι ειδοποιήσεις μπορούν είτε να αποστέλλονται στο syslog, είτε να καταγράφονται σε ένα αρχείο κειμένου ειδοποίησης σε δύο διαφορετικές μορφές. Οι ειδοποιήσεις syslog αποστέλλονται ως ασφάλεια και εξουσιοδότηση σε μηνύματα που παρακολουθούνται. Οι ειδοποιήσεις επιτρέπουν την αποστολή ειδοποιήσεων και συμβάντων σε μια λίστα. Υπάρχει η πλήρης ειδοποίηση οπου γράφει μήνυμα ειδοποίησης και τις πληροφορίες κεφαλίδας πακέτου μέσω του πρωτοκόλλου του επιπέδου μεταφοράς και υπάρχει και η γρήγορη ειδοποίηση οπου γράφει ένα συμπυκνωμένο υποσύνολο των πληροφοριών κεφαλίδας στο αρχείο ειδοποίησης, επιτρέποντας μεγαλύτερη απόδοση υπό φορτίο παρά σε πλήρη λειτουργία. Υπάρχει μια άλλη επιλογή για να απενεργοποιήστε πλήρως την ειδοποίηση, η οποία είναι χρήσιμη όταν η ειδοποίηση είναι περιττή ή ακατάλληλη, όπως όταν πραγματοποιούνται δοκιμές διείσδυσης δικτύου. Επίσης οι ειδοποιήσεις είναι κάθε είδους ειδοποίηση χρήστη για μια δραστηριότητα εισβολέα και όταν ανιχνεύει ένα IDS ένας εισβολέας, πρέπει να ενημερώσει τον διαχειριστή ασφαλείας σχετικά με αυτό χρησιμοποιώντας ειδοποιήσεις. Οι ειδοποιήσεις μπορεί να είναι με τη μορφή αναδυόμενων παραθύρων, σύνδεσης σε μια κονσόλα, αποστολής email. Ειδοποιήσεις αποθηκεύονται επίσης σε αρχεία καταγραφής ή βάσεις δεδομένων όπου μπορούν να προβληθούν αργότερα από την ασφάλεια ειδικοί. Θα βρείτε λεπτομερείς πληροφορίες σχετικά με τις

ειδοποιήσεις αργότερα σε αυτό το βιβλίο. Το Snort μπορεί να δημιουργήσει ειδοποιήσεις σε πολλές μορφές και ελέγχεται από πρόσθετα εξόδου. Το Snort μπορεί επίσης να στείλει την ίδια ειδοποίηση σε πολλούς προορισμούς. Για παράδειγμα, είναι δυνατό να καταγραφή ειδοποιήσεων σε μια βάση δεδομένων και δημιουργία παγίδων SNMP ταυτόχρονα. Ορισμένα πρόσθετα μπορούν τροποποιήστε επίσης τη διαμόρφωση του τείχους προστασίας έτσι ώστε οι προσβλητικοί κεντρικοί υπολογιστές να αποκλείονται στο τείχος προστασίας ή επίπεδο δρομολογητή.

Επίσης στο snort οι υπογραφές(signatures) είναι μοναδικά χαρακτηριστικά ενός πακέτου που το προσδιορίζουν ως επικίνδυνο και πρόκειται για μοτίβα από συμβολοσειρές που χαρακτηρίζονται ως υπογραφή ενός κακού πακέτου και βρίσκονται στο ωφέλιμο φορτίο ή στην κεφαλίδα του πακέτου. Όταν χρησιμοποιείτε μια υπογραφή, η γενική περιγραφή ενός κακόβουλου πακέτου είναι στατική. Δηλαδή, μια υπογραφή περιγράφει μια ιδιότητα ωφέλιμου φορτίου και ορισμένα στοιχεία κεφαλίδας πακέτου. Η υπογραφή είναι το μοτίβο που αναζητάτε μέσα σε ένα πακέτο δεδομένων. Χρησιμοποιείται υπογραφή για τον εντοπισμό ενός ή πολλαπλών τύπων επιθέσεων. Οι υπογραφές μπορεί να υπάρχουν σε διαφορετικά μέρη ενός πακέτου δεδομένων ανάλογα με το φύση της επίθεσης. Για παράδειγμα, μπορείτε να βρείτε υπογραφές στην κεφαλίδα IP, μεταφορά επικεφαλίδα επιπέδου TCP ή UDP και στην κεφαλίδα επιπέδου εφαρμογής ή στο ωφέλιμο φορτίο. Συνήθως το IDS εξαρτάται από τις υπογραφές για να ενημερωθεί για τη δραστηριότητα του εισβολέα

Επίσης μία από τις πιο κρίσιμες πτυχές των συστημάτων ανίχνευσης εισβολής είναι και οι κανόνες(rules). Οι κανόνες είναι ένα πρότυπο με το οποίο μπορείτε να αναζητήσετε σε κινούμενα πακέτα του δικτύου σας. Η εύρεση ενός πακέτου με χαρακτηριστικά που είναι πανομοιότυπα με αυτά του προτύπου θεωρείται επίθεση από το λογισμικό. Μπορεί να εντοπίσει μια προσπάθεια σύνδεσης από μια ύποπτη IP ελέγχοντας τη διεύθυνση πηγής με ένα ασυνήθιστο συνδυασμό πακέτων TCP. Ακόμη μπορεί να προσδιορίσει μια επίθεση Dos χρησιμοποιώντας διάφορες μεθόδους παροχής της ίδιας εντολής, η οποία αντιμετωπίζεται μετρώντας τον αριθμό των φορών που εκτελείται μια εντολή και δημιουργώντας συναγερμό όταν ξεπεραστεί το καθορισμένο όριο. Ακόμη μπορεί να εντοπίσει μια επίθεση σε έναν διακομιστή FTP δημιουργώντας μια υπογραφή που βασίζεται σε μια σειρά καταστάσεων δηλαδή παρακολούθηση σταδίου και

προειδοποιώντας όταν κάποιος προσπαθεί να κάνει μια κίνηση χωρίς να ακολουθήσει το κατάλληλο πρωτόκολλο. Επίσης εξετάζοντας απλώς το όνομα του θέματος ή των συνημμένων, ο σχετικός κανόνας μπορεί να εντοπίσει ένα ηλεκτρονικό μήνυμα όπου μπορεί να περιέχει κάποιο ιό.

Τα μηνύματα καταγραφής logs αποθηκεύονται συνήθως σε αρχείο και από προεπιλογή, το Snort αποθηκεύει αυτά τα μηνύματα στον κατάλογο. Ωστόσο, η θέση των μηνυμάτων καταγραφής μπορεί να αλλάξει χρησιμοποιώντας το διακόπτη γραμμής εντολών κατά την εκκίνηση του Snort. Τα μηνύματα καταγραφής μπορούν να αποθηκευτούν είτε σε μορφή κειμένου ή δυαδικής μορφής. Τα δυαδικά αρχεία μπορούν να προβληθούν αργότερα χρησιμοποιώντας το Snort ή το tcpdump πρόγραμμα. Ένα νέο εργαλείο που ονομάζεται barnyard είναι επίσης διαθέσιμο τώρα για την ανάλυση δυαδικών αρχείων καταγραφής που δημιουργήθηκε από το Snort. Η σύνδεση σε δυαδική μορφή είναι πιο γρήγορη επειδή αποθηκεύει κάποια μορφοποίηση πάνω από το κεφάλι. Σε εφαρμογές Snort υψηλής ταχύτητας, η σύνδεση σε δυαδική λειτουργία είναι απαραίτητη.

Τέλος το Snort είναι ένα ευέλικτο εργαλείο με μεγάλη ποικιλία χρήσεων. Προορίζεται να χρησιμοποιηθεί με την πιο κλασική έννοια ενός συστήματος ανίχνευσης εισβολής δικτύου. Εξετάζει την κυκλοφορία του δικτύου σε σχέση με ένα σύνολο κανόνων και ειδοποιεί τους διαχειριστές για ύποπτη δραστηριότητα δικτύου, ώστε να αντιδράσουν κατάλληλα. Υπάρχουν πολλοί άλλοι τομείς όπου το Snort μπορεί επίσης να είναι χρήσιμο. Το Snort σχεδιάστηκε για να εκπληρώνει τις απαιτήσεις ενός πρωτότυπου ελαφρού συστήματος ανίχνευσης εισβολών δικτύου. Έχει γίνει ένα μικρό, ευέλικτο και εξαιρετικά ικανό σύστημα που χρησιμοποιείται σε όλο τον κόσμο τόσο σε μεγάλα όσο και σε μικρά δίκτυα. Έχει φτάσει στο αρχικό του σχεδιαστικών στόχων και είναι μια πλήρως ικανή εναλλακτική λύση στα εμπορικά συστήματα ανίχνευσης εισβολής σε μέρη όπου η εγκατάσταση εμπορικών συστημάτων με πλήρη χαρακτηριστικά δεν είναι αποδοτική.

References:

http://apothesis.teicm.gr/xmlui/bitstream/handle/123456789/786/zounarakis.pdf?sequence=1&isAllowed=y

http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/5824/Roussos.pdf?sequence=2&isAllowed=y

http://estia.hua.gr/file/lib/default/data/22319/theFile

https://nemertes.lis.upatras.gr/jspui/bitstream/10889/13158/3/Nemertes_Ntourampas%28com%29.pdf