Ασφάλεια Συστημάτων και Υπηρεσιών - ΗΡΥ 413

Αστερινός Καράλης – Ζωγραφούλα Ιωάννα Νεαμονιτάκη

Part 6

Describe how Snort uses rules to detect malicious activity.

Το Snort αναλύει πακέτα και τα συγκρίνει με ένα set από κανόνες που μπορούν να περιγράφουν κακόβουλη ή ύποπτη συμπεριφορά. Αυτοί οι κανόνες μπορούν να περιγράφουν γνωστά κακόβουλα αρχεία, δηλαδή συγκεκριμένο περιεχόμενο μέσα στα πακέτα, το port στο οποίο στέλνονται ή και συγκεκριμένο μέγεθος των πακέτων, ή πρωτοκολλά που χρησιμοποιούν. Άρα όταν οι κανόνες εντοπίσουν κάποιο ύποπτο πακέτο, το Snort μπορεί είτε να πετάξει κάποιο alert, είτε να μπλοκάρει το πακέτο, να αλλάξει το πακέτο ή και να στείλει μία απάντηση.

Mention at least 6 limitations of signature-based intrusion detection systems like Snort with a small description for each one.

Όλα τα συστήματα που θα αναλυθούν είναι Intrusion Detection and Prevention Systems (IDPS)

1. Palo Alto Networks Next-Generation Firewalls

Το Palo Alto Firewalls ταξινομεί όλη το traffic, συμπεριλαμβανομένου του κρυπτογραφημένου traffic, με βάση την εφαρμογή, τη λειτουργία εφαρμογής, τον χρήστη και το περιεχόμενο. Μπορεί να δημιουργήσει ολοκληρωμένες, ακριβείς πολιτικές ασφαλείας, με αποτέλεσμα την ασφαλή ενεργοποίηση των εφαρμογών. Αυτό επιτρέπει να εκτελούν μόνο εξουσιοδοτημένοι χρήστες συγκεκριμένες εφαρμογές, μειώνοντας σημαντικά τα cyber attacks.

1. Ossec

Το Ossec είναι ένα open source host-based intrusion detection system που εκτελεί ανάλυση αρχείων καταγραφής, έλεγχο ακεραιότητας αρχείων, παρακολούθηση πολιτικής, ανίχνευση rootkit και παρακολούθηση διεργασιών.

1. CrowdSec

Το CrowdSec είναι ένα συνεργατικό open source intrusion detection system που βασίζεται στην συμπεριφορά μιας IP και του reputation της. Όταν το CrowdSec βρει κακόβουλη συμπεριφορά τότε μοιράζεται την IP με το community του για να επιτρέψει σε όλους να την κάνουν block.

1. AlienVault USM (from AT&T Cybersecurity)

Το AlienVault USM (from AT&T Cybersecurity) είναι μια πλατφόρμα που παρέχει πέντε βασικές δυνατότητες ασφάλειας σε ένα ενιαίο console με στόχο της διαχείριση των απειλών, κατανοώντας τo sensitive nature των IT περιβαλλόντων παρέχοντας active, passive και host-based τεχνολογίες.

1. Security Onion

Security Onion είναι ένα Linux distro για intrusion detection, network security monitoring, και log management, το οποίο μπορεί να κάνει monitor και τον host αλλά και το network.

1. Suricata

To Suricata είναι open-source intrusion detection system και intrusion prevention system. Είναι η κύρια εναλλακτική του Snort καθώς είναι συμβατό με τους κανόνες και τα Snort fortmats. Το σημαντικό του πλεονέκτημα ενάντια στο Snort είναι ότι συλλέγει τα δεδομένα στο application layer.

Pros and cons of using Snort in a real-world scenario

Κάποια από τα πλεονεκτήματα του Snort:

* Open-Source, το οποίο σημαίνει πως είναι δωρεάν.
* Προσαρμοστικότητα, ο καθένας μπορεί να φτιάξει custom rules για τις ανάγκες του.
* Ανάλυση πραγματικού χρόνου, το οποίο είναι και το ζητούμενο σε ένα πραγματικό σενάριο.
* Υπάρχει μεγάλο community support.
* Το Snort υποστηρίζεται και από Linux κι από windows

Κάποια Μειονεκτήματα:

* Όπως είδαμε και από το μέρος 5, το Snort για πολύ μεγάλα αρχεία χρειάζεται αρκετούς πόρους και έχει μεγάλο CPU usage.
* Παρόλου που υπάρχει community support, δεν υπάρχει κάποιο συγκεκριμένο customer support.
* Επειδή είναι signature-based το snort δεν μπορεί να προλάβει κάποια νέα απειλή, μόνο τις γνωστές δηλαδή μπορεί να «πιάσει»
* Το Snort μπορεί να δυσκολευτεί σε περίπλοκα περιβάλλοντα και μεγάλα δίκτυα, λόγο του πρώτου bullet.