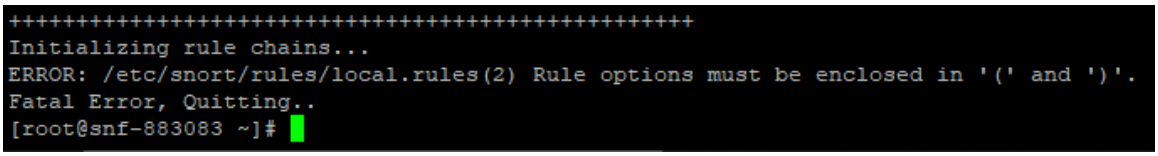
Ασφάλεια Δικτύων

Εργαστηριακή Άσκηση 2 (Snort)

Διογένης Τσολάκου - 3170164

Server IP : 83.212.110.24

Δυστυχώς κατά τη διάρκεια της εκτέλεσης της εντολής του snort έβγαζε error το οποίο δεν μπορώ να αντιληφθώ για ποιο λόγο βγαίνει το συγκεκριμένο error μιας και έχω χρησιμοποιήσει παρενθέσεις για τα options των κανόνων.



1)

alert icmp any any -> 83.212.110.24 any (msg:"Ping scan detected"; sid:10000001; rev:001;)

Χρησιμοποιήθηκε ο συγκεκριμένος κανόνας καθώς ένα ping scan στέλνει ICMP πακέτα. Επιπλέον αφού θέλουμε να ανιχνεύσουμε ping στον server μας στην destination IP address ορίστηκε η IP του VM στον okeanos.

2)

alert ip any any -> any [80, 443] (content:"admin@site.gr";msg:"Http/https scan detected!";flags:S; sid:10000002; rev:001;)

Επειδή θέλουμε να ανιχνεύσουμε πακέτο γενικά προς http/https ports στο πρωτόκολλο έβαλα ip και στον ορισμό των ports έβαλα λίστα από τα ports του καθενός, 80 για http και 443 για https. Μιας και γνωρίζουμε ότι το συγκεκριμένο

πακέτο έχει payload το <<admin@site.gr>> χρησιμοποιήθηκε η παράμετρος content ώστε να οριστεί το payload. Τέλος, αφού δεν θέλουμε να ανιχνεύσουμε μόνο πακέτα προς τον server μας χρησιμοποιήθηκε η παράμετρος any στο destination IP address.

3)

alert tcp any any -> 83.212.110.24 [!80, !443, !21, !22] (msg:"NMAP Fast Scan";flags:S; threshold:type limit, track by_dst, count 10; sid:10000003; rev:001;)

Καθώς γίνεται port scan προς τον server όρισα ως πρωτόκολλο το TCP και ως destination IP address την IP του VM. Επίσης, αφού θέλουμε οι συνδέσεις σε http, https, ftp και ssh να θεωρηθούν ως φυσιολογικές όρισα ως destination port τη λίστα των συγκεκριμένων πρωτοκόλλων με negation, δηλαδή με θαυμαστικό, ώστε να μην βγάλει alert για πακέτα TCP προς αυτά τα ports. Αφού γίνεται fast scan με TCP βάζουμε στα flags το S (SYN). Τέλος, αφού θέλουμε να εμφανίζονται το πολύ 10 alerts σε κάθε scan όρισα την παράμετρο threshold με τις επιλογές type limit, track by_dst ώστε να γίνεται track ανάλογα με τα πακέτα που κατευθύνονται προς την destination IP και με count 10.

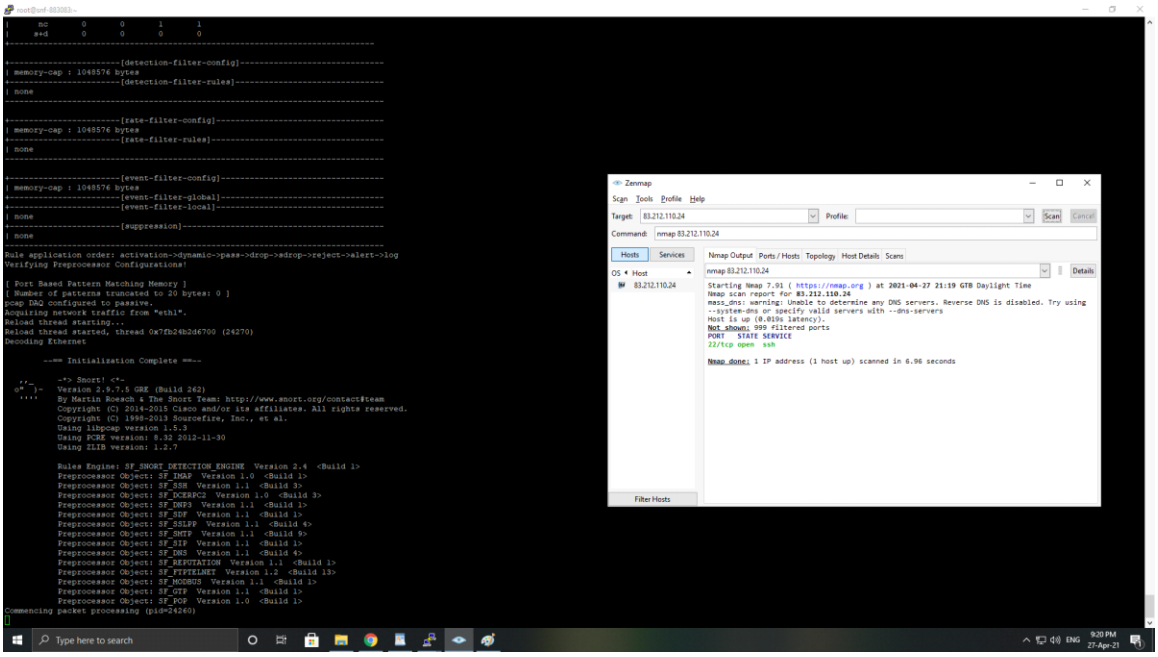
4)

alert ip any any -> 195.251.248.0/21 any (msg:"AUEB IP Scan"; sid:10000004; rev:001;)

Επειδή θέλουμε να ανιχνεύσουμε οποιαδήποτε κίνηση προς το IP range του ΟΠΑ, ορίστηκε ως πρωτόκολλο το ip και ως destination IP το 195.251.248.0/21.

Α) Ο συγκεκριμένος κανόνας pass αγνοεί κάθε πακέτο μιας και έχει ως πρωτόκολλο ip, source IP, source port any και destination IP, destination source any. Οπότε όπως φαίνεται στο παρακάτω screenshot δεν εμφανίζει κάποιο alert.

Χρησιμοποιήθηκε ο test κανόνας που είχε δοθεί αρχικά.



B) Ο συγκεκριμένος κανόνας μπλοκάρει και καταγράφει πακέτα με πρωτόκολλο TLS τα οποία προέρχονται από ένα εξωτερικό δίκτυο ορισμένο στο conf αρχείο του Snort με όνομα μεταβλητής EXTERNAL_NET και κατευθύνεται προς το τοπικό δίκτυο που είναι κι αυτό ορισμένο στο conf με όνομα HOME_NET. Τυπώνει το ορισμένο μήνυμα μέσα στα quotes. Επιπλέον αυτά τα πακέτα πρέπει να έχουν το ορισμένο fingerprint σύφωνα με το site που ορίζεται στο reference, το οποίο site

ανιχνεύει και κάνει blacklist κακόβουλα SSL certificates.

Επομένως, ουσιαστικά ο κανόνας μπλοκάρει πακέτα που έχουν ως σκοπό την προσπάθεια εγκαθίδρυσης SSL σύνδεσης και προέρχονται από command & control servers που ελέγχουν κάποιο botnet.