Δρ. Μαριάς Ιωάννης
Επικ. Καθηγητής

Προπτυχιακό Πρόγραμμα Σπουδών
Εαρινό εξάμηνο 2020-2021

Ασφάλεια Δικτύων
Εργαστηριακή Άσκηση 2 (snort)

Εκτελείτε το snort για προετοιμασία με την εντολή:
sudo snort -A console -i eth1 -c /etc/snort/snort.conf

Την ώρα των επιθέσεων για να καταγραφεί και σε log file πέρα από τα alerts που θα εμφανίζονται στην κονσόλα με την εντολή:
sudo snort -A console -i eth1 -c /etc/snort/snort.conf |& tee -a /root/snort_log.txt

1) Προσθέστε τον κατάλληλο κανόνα (alert) στο /etc/snort/rules/local.rules προκειμένου να ανιχνεύσετε ping προς τον server σας.
Σχολιάστε αν βρεθούν αποτελέσματα. (copy ή screenshot από τα alerts)
Δικαιολογήστε τον κανόνα που χρησιμοποιήσατε.

2) Προσθέστε τον κατάλληλο κανόνα (alert) στο local.rules προκειμένου να ανιχνεύσετε πακέτο προς http/https ports και περιλαμβάνει (payload) το «admin@site.gr».
Σχολιάστε αν βρεθούν αποτελέσματα. (copy ή screenshot από τα alerts)
Δικαιολογήστε τον κανόνα που χρησιμοποιήσατε.

3) Προσθέστε τον κατάλληλο κανόνα (alert) στο local.rules προκειμένου να ανιχνεύσετε port scan προς τον server σας (θα γίνει nmap fast scan).
Θεωρήστε ότι http, https, ftp, ssh συνδέσεις είναι φυσιολογικές.
Βεβαιωθείτε ότι εμφανίζονται ελάχιστα alerts (max 10) σε κάθε scan
Σχολιάστε αν βρεθούν αποτελέσματα. (copy ή screenshot από τα alerts)
Δικαιολογήστε τον κανόνα που χρησιμοποιήσατε.

4) Προσθέστε τον κατάλληλο κανόνα (alert) στο local.rules προκειμένου να ανιχνεύσετε κίνηση προς το ip range του ΟΠΑ (195.251.248.0 /21) .
Σχολιάστε αν βρεθούν αποτελέσματα. (copy ή screenshot από τα alerts)
Δικαιολογήστε τον κανόνα που χρησιμοποιήσατε.

Στο report απαντήστε και τις ακόλουθες ερωτήσεις:

Α) Αν προστεθεί ο παρακάτω κανόνας τι επίδραση θα έχει στους δικούς σας;

```
pass ip any any -> any any (msg:"Allowed";sid:1001;)
```

Β) Εξηγείστε πως λειτουργεί ο παρακάτω κανόνας:

```
drop tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSLBL: Malicious SSL
certificate detected (Malware C&C)";
tls.fingerprint:"91:a4:7b:29:99:12:f1:20:4f:db:e2:97:4e:27:26:2b:f8:9a:0a:06";
reference:url, sslbl.abuse.ch/ssl-
certificates/sha1/91a47b299912f1204fdbe2974e27262bf89a0a06/;
sid:902202603; rev:1;)
```

Οι αναφερόμενες «επιθέσεις» θα πραγματοποιηθούν μεταξύ 18:45 και 18:55

Το sid του κάθε κανόνα πρέπει να αντιστοιχεί εμφανώς στον αριθμό του ζητούμενου/εκφώνησης. Σχολιάστε τα αποτελέσματα σε κάθε alert που εμφανίζεται.

Υποβάλετε το περιεχόμενο του local.rules όπως έχει διαμορφωθεί στο eclass (κατάλογος Εργασίες) μέχρι 19:00
Αναρτήστε τις απαντήσεις σας, screenshot ή copy από τα alerts που εμφανίστηκαν στο eclass (κατάλογος Εργασίες) μέχρι 23:55