Ασφάλεια Δικτύων

Εργαστηριακή Άσκηση 2

Φίλιππος Δουραχαλής, 3170045

Η IP του υπολογιστή μας είναι η 83.212.110.51

Η μεταβλητή $HOME_NET στο αρχείο snort.conf έχει οριστεί να είναι η διεύθυνση του server μας.

```
# Step #1: Set the network variables.  For more information, see README.variables
#####################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 83.212.110.51
```

1) alert icmp any any -> $HOME_NET any (msg:"Ping request detected"; sid:10000001; rev:001;)

Μερικά από τα ICMP Echo requests και replies που παρατηρήθηκαν από και προς τον server μας είναι τα εξής:

```
04/27-12:47:51.645160  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:47:51.762162  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 209.141.46.206:51140 -> 83.212.110.51:443
04/27-12:47:51.762333  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 209.141.46.206
04/27-12:47:54.432993  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 195.251.255.77 -> 83.212.110.51
04/27-12:47:54.433218  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 195.251.255.77
04/27-12:47:54.433302  [**] [1:10000002:1] HTTP/HTTPS packet sent to admin@site.gr [**] [Priority: 0] {TCP} 195.251.255.77:52511 -> 83.212.110.51:443
04/27-12:47:54.433302  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 195.251.255.77:52511 -> 83.212.110.51:443
04/27-12:47:54.433375  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 195.251.255.77
04/27-12:47:54.436705  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 195.251.255.77 -> 83.212.110.51
04/27-12:47:54.436814  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 195.251.255.77
04/27-12:47:57.086006  [**] [1:10000002:1] HTTP/HTTPS packet sent to admin@site.gr [**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.51:80
04/27-12:47:57.086006  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.51:80
04/27-12:47:57.086235  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 195.251.255.77
04/27-12:47:57.127006  [**] [1:10000002:1] HTTP/HTTPS packet sent to admin@site.gr [**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.51:443
04/27-12:47:57.127006  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.51:443
04/27-12:47:57.127136  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 195.251.255.77
```

Τα αποτελέσματα περιλαμβάνουν requests προς την διεύθυνση 83.212.110.86, αλλά και requests και replies μεταξύ του μηχανήματός μας και της διεύθυνσης 195.251.255.77

Ο κανόνας ενεργοποιείται για όλα τα ICMP πακέτα που αποστέλλονται από οποιαδήποτε διεύθυνση και από οποιαδήποτε θύρα στις διευθύνσεις που ορίζει η μεταβλητή $HOME_NET.

2) alert tcp any any <> $HOME_NET [80,443] (msg:"HTTP/HTTPS packet sent to admin@site.gr"; content:"admin@site.gr"; sid:10000002; rev:001;)

Καταγράφηκαν τα εξής 3 πακέτα που αφορούν κίνηση HTTP και HTTPS από έναν απομακρυσμένο υπολογιστή προς τον server. Παρατηρούμε ότι το πρώτο και τελευταίο πακέτο είναι ένα μήνυμα HTTPS, ενώ το δεύτερο αφορά ένα απλό μήνυμα HTTP:

i. 04/27-12:47:57.127006 [**] [1:10000002:1] HTTP/HTTPS packet sent to admin@site.gr [**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.51:443

ii. 04/27-12:47:57.086006 [**] [1:10000002:1] HTTP/HTTPS packet sent to admin@site.gr [**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.51:80

iii. 04/27-12:47:54.433302 [**] [1:10000002:1] HTTP/HTTPS packet sent to admin@site.gr [**] [Priority: 0] {TCP} 195.251.255.77:52511 -> 83.212.110.51:443

Ο κανόνας εμφανίζει προειδοποιητικό μήνυμα για τα TCP πακέτα που στέλνονται προς τις θύρες 80 και 443 του server (που αντιστοιχούν στις υπηρεσίες HTTP και HTTPS), αλλά και για τα πακέτα που στέλνει το μηχάνημά μας από τα συγκεκριμένα ports προς οποιαδήποτε διεύθυνση και θύρα. Επίσης μέσω του option “content” ορίζουμε ότι τα παραπάνω πακέτα θα πρέπει να περιέχουν στο payload την ακολουθία (pattern) “admin@site.gr”.

3) alert tcp any any <> $HOME_NET ![21,22,80,443] (msg:"Nmap scan detected"; sid:10000003; rev:001;)

Στην παρακάτω εικόνα παρατηρούμε μερικά από τα πακέτα που στέλνονται προς διάφορες TCP θύρες του υπολογιστή μας, πιθανώς ως αποτέλεσμα ενός port scan.

```
04/27-12:47:58.846765  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40741 -> 83.212.110.51:22
04/27-12:47:58.847004  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.51:22 -> 83.212.110.86:40741
04/27-12:47:58.847773  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40741 -> 83.212.110.51:22
04/27-12:48:04.283225  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 185.193.88.29:46523 -> 83.212.110.51:12500
04/27-12:48:04.283431  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 185.193.88.29
04/27-12:48:07.244423  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40729 -> 83.212.110.51:113
04/27-12:48:07.244629  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:48:07.444863  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40729 -> 83.212.110.51:110
04/27-12:48:07.445063  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:48:07.644802  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40729 -> 83.212.110.51:445
04/27-12:48:07.645007  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:48:07.831450  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40730 -> 83.212.110.51:445
04/27-12:48:07.831654  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:48:07.844461  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40729 -> 83.212.110.51:143
04/27-12:48:07.844577  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:48:07.988703  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40730 -> 83.212.110.51:143
04/27-12:48:07.988878  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:48:08.121061  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 61.177.173.3:51452 -> 83.212.110.51:22
04/27-12:48:08.121270  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.51:22 -> 61.177.173.3:51452
04/27-12:48:08.445154  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40729 -> 83.212.110.51:139
04/27-12:48:08.445356  [**] [1:10000001:1] Ping request detected [**] [Priority: 0] {ICMP} 83.212.110.51 -> 83.212.110.86
04/27-12:48:08.557143  [**] [1:10000003:1] Nmap scan detected [**] [Priority: 0] {TCP} 83.212.110.86:40730 -> 83.212.110.51:139
```

Σε ένα fast scan, το nmap στέλνει πακέτα TCP στις 100 πιο γνωστές θύρες. Επομένως πρέπει να εντοπίσουμε αυτά τα tcp πακέτα που στέλνονται προς την IP μας, εξαιρώντας όμως τα πακέτα που έχουν ως θύρα προορισμού μια από τις γνωστές θύρες 21 (FTP), 22 (SSH), 80 (HTTP) και 443 (HTTPS), αφού θεωρούμε ότι οι συνδέσεις αυτές είναι φυσιολογικές. Επίσης με τον τελεστή “<>” εντοπίζουμε και την tcp κίνηση που αποστέλλεται από τον υπολογιστή μας από κάποιο port εκτός

των παραπάνω, επειδή το πακέτο που στέλνεται μπορεί να είναι απάντηση σε κάποιο πακέτο του port scan.

4) alert ip $HOME_NET any -> 195.251.248.0/24 any (msg:"Packets sent to 195.251.248.0/24 detected"; sid:10000004; rev:001;)

Δεν παρατηρήθηκαν αποτελέσματα εφαρμογής του συγκεκριμένου κανόνα.

Ο κανόνας προειδοποιεί για κάθε IP πακέτο (και άρα για κάθε πακέτο ανώτερου επιπέδου που ενθυλακώνεται σε αυτό) που αποστέλλεται από την διεύθυνση του μηχανήματός μας σε οποιαδήποτε διεύθυνση εντός του δικτύου του πανεπιστημίου (195.251.248.0/21), άρα εμφανίζει μήνυμα για οποιουδήποτε είδους κίνηση προς το ΟΠΑ.

Σημείωση: Για τους κανόνες 1-3 θα μπορούσαμε να είχαμε θέσει ως διεύθυνση προέλευσης την “!$HOME_NET” ώστε να αποκλείσουμε κίνηση που ενδεχομένως να στέλνει ο server στον εαυτό του.

A) Ο κανόνας “pass ip any any ->any any (msg:"Allowed";sid:1001;)” λέει στο Snort να αγνοήσει όλα τα ip πακέτα, ανεξαρτήτου διεύθυνσης και θύρας. Άρα ενεργοποιείται για όλα τα πακέτα, όμως δεν έχει επίδραση σε κάποιον από τους παραπάνω κανόνες διότι η προτεραιότητα των κανόνων alert είναι μεγαλύτερη από αυτή των κανόνων pass. Αυτό σημαίνει πως το Snort πρώτα θα εξετάσει τους κανόνες alert και θα τους αντιστοιχίσει ενδεχομένως στο πακέτο, και έπειτα θα ελέγξει τους κανόνες pass, επομένως αν ενεργοποιηθεί κάποιο alert θα εμφανιστεί στην κοσνόλα ανεξαρτήτως.

B) 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;)

Ο κανόνας εξετάζει μηνύματα που στέλνονται από servers κατά τη διαδικασία του TLS Handshake και που περιέχουν ένα συγκεκριμένο TLS Certificate. Όταν προκύψει αντιστοίχιση με κάποιο πακέτο, αυτό απορρίπτεται. Ο κανόνας ενεργοποιείται για πακέτα τα οποία αποστέλλονται από τις διευθύνσεις ενός εξωτερικού δικτύου, που ορίζονται με τη μεταβλητή EXTERNAL_NET, προς τις διευθύνσεις στο δίκτυο μας, οι οποίες με τη σειρά τους προσδιορίζονται με τη μεταβλητή HOME_NET. Επιπλέον, ελέγχει αν το πιστοποιητικό που λαμβάνουμε είναι κάποιο γνωστό blacklisted πιστοποιητικό, που προσδιορίζεται από το URL της επιλογής “reference”, και αν το

αποτύπωμά του είναι το SHA-1 hash αποτύπωμα πιστοποιητικού που δίνεται στην επιλογή “tls.fingerprint”.

Γενικά ο κανόνας απορρίπτει μηνύματα που φέρουν το παραπάνω πιστοποιητικό, επειδή αυτό συσχετίζεται με κακόβουλους servers και άρα είναι αναξιόπιστο.