**Ασφάλεια συστημάτων και υπηρεσιών**

Project 7

Αμπλιανίτης Κωνσταντίνος

2017030014

## Πίνακας κάνονων για το firewall

| Action | Source Address | Dest. Address | Protocol | Source Port | Dest. Port | Flag Bit | Check Connection | Descr* |
|---|---|---|---|---|---|---|---|---|
| Allow | TUC | Internet | TCP | >1023 | 22 | any | | 1 |
| Allow | Internet | TUC | TCP | 22 | >1023 | ACK | ✗ | 2 |
| Allow | Internet | TUC | TCP | >1023 | 80 | any | | 3 |
| Allow | TUC | Internet | TCP | 80 | >1023 | ACK | ✗ | 4 |
| Allow | Internet | TUC | TCP | >1023 | 443 | any | | 3 |
| Allow | TUC | Internet | TCP | 443 | >1023 | ACK | ✗ | 4 |
| Allow | Internet | TUC | UDP | 53 | >1023 | any | ✗ | 5 |
| Allow | TUC | Internet | UDP | >1023 | 53 | any | | 6 |
| Allow | Internet | TUC | TCP | 53 | >1023 | ACK | ✗ | 7 |
| Allow | TUC | Internet | TCP | >1023 | 53 | any | | 8 |
| Reject | Internet | TUC | ICMP | - | - | any | | 9 |
| Allow | TUC | Internet | ICMP | - | - | any | | 10 |
| Deny | all | all | all | all | all | all | | 11 |

Descr*: Κάθε αριθμός αντιστοιχεί σε μία εξήγηση παρακάτω

**Description:**

**1.** Δεδομένου ότι τόσο το ssh, το sftp όσο και όλες οι υπηρεσίες που τρέχουν πάνω σε αυτά είναι σε TCP και ακούν στο port 22 υπάρχει ο κανόνας 1.

**2.** Καθώς μόνο οι εσωτερικοί χρήστες μπορούν να περιηγούνται σε εξωτερικούς ιστοτόπους, δεν γίνεται να έρθουν πακέτα aknowledge όποτε σε τέτοια περίπτωση η σύνδεση κόβεται.

**3.** Εξωτερικοί χρήστες μπορούν να έχουν πρόσβαση στον web-server του Π.Κ. Ως web-server τα known ports είναι τα 80 ή 443.

**4.** Δεδομένης της δομής του TCP σε περίπτωση που πακέτα ACK φεύγουν από τον server του Π.Κ. θα πρέπει να κόβεται η σύνδεση για λόγους ασφαλείας.

**5.** Λόγω πολύ εύκολου exploitation του DNS μέσω UDP από το port 53 αποκλείονται όλες οι συνδέσεις από εξωτερικούς χρήστες προς το εσωτερικό για λόγους ασφαλείας (ευκολία να γίνουν επιθέσεις DDOS).

**6.** Αναζήτηση πληροφοριών DNS μέσω UDP protocol από τους εσωτερικούς χρήστες προς εξωτερικούς ιστοτόπους.

**7.** Αναζήτηση πληροφοριών DNS μέσω TCP protocol από τους εξωτερικούς χρήστες προς το εσωτερικό. Λόγω της δομής του TCP, packets όπου αποστέλονται ως ACK οδηγούν σε διακοπή σύνδεσης για λόγους ασφαλείας.

**8.** Αναζήτηση πληροφοριών DNS από εσωτερικούς χρήστες προς το εξωτερικό.

**9.** Απόριψη όλων των εξωτερικών πακέτων προς τον web-server του Π.Κ.

**10.** Αποστολή πακέτων από τους εσωτερικούς χρήστες προς οπουδήποτε εκτός του Π.Κ.

**11.** Άρνηση όλων των υπόλοιπων πακέτων οποιουδήποτε πρωτοκόλου που δεν ανήκουν στις παραπάνω κατηγορίες.

## Ερώτημα 2

Σε περίπτωση προσπάθειας υλοποίησης του συγκεκριμένου firewall σε ένα Linux Pc θα απαιτούνταν δύο ethernet κάρτες. Μία για σύνδεση στο διαδύκτιο και μία με σκοπό να χρησιμοποιήθει το PC σαν ένα hardware firewall για τις συσκευές που θα υπάρχουν μέσα στο Π.Κ.

**Βιβλιογραφία:**

Ασφάλεια Υπολογιστών Αρχές και πρακτικές || William Stallings, Lawrie Brown

Computer Networking A Top-Down Approach || KUROSE ROSS

https://forums.tomshardware.com/threads/why-does-my-mobo-have-2-ethernet-ports.1759734/

https://www.chegg.com/homework-help/questions-and-answers/provide-stateful-filter-table-connection-table-stateful-firewall-restrictive-possible-acco-q48545911