*[ΗΡΥ\_414] ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ*

*Διδάσκων: Σωτήριος Ιωαννίδης Εργαστήριο: Κ. Παπαδημητρίου, Σ. Μπούρος*

*ΑΣΚΗΣΗ 7: TUC Firewall*

*Κατσίμπας Πέτρος*

*2016030038*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Action*** | ***Source Address*** | ***Dest address*** | ***Protocol*** | ***Source port*** | ***Dest port*** | ***Flag Bit*** | ***Check connection*** | ***Description*** |
| ALLOW | TUC | Internet | TCP | 22 | \*\*\* | Any |  |  |
| ALLOW | Internet | TUC | TCP | \*\*\* | 80/443 | Any |  |  |
| ALLOW | TUC | Internet | TCP/UDP\* | 53 | \*\*\* | Any/-\* |  |  |
| ALLOW | Internet | TUC | TCP/UDP\* | \*\*\* | 53 | Any/-\* |  |  |
| REJECT | Internet | TUC | ICMP | \*\*\* | 80/443 | Any |  |  |
| ALLOW | TUC | Internet | ICMP | 80/443 | \*\*\* | Any |  |  |
| DENY | TUC | Internet | TCP | 22 | \*\*\* | Any | **X** |  |
| DENY | Internet | TUC | TCP | \*\*\* | 22 | Any | **X** |  |

*Για την 7η εργαστηριακή άσκηση συμπληρώσαμε τον πίνακα όπως μας ζητήθηκε. Σύμφωνα με τις πολιτικές του τείχους προστασίας που αναγράφονταν στην εκφώνηση αλλά και την βοηθητική βιβλιογραφία έχουμε ως εξής:*

\*Κατά κύριο λόγο το DNS αποτελεί UDP πρωτόκολλο, όμως παρατηρείται να χρησιμοποιεί σε αρκετές περιστάσεις TCP αφού το σταλμένο πακέτο ξεπερνάει τα 512-bits.( <https://www.infoblox.com/dns-security-resource-center/dns-security-faq/is-dns-tcp-or-udp-port-53/> ) Έτσι, εξίσου για τον λόγο αυτό δεν είμαστε σίγουροι εάν το FLAG\_BIT θα είναι any λόγω TCP ή κενό λόγω connectionless UDP πρωτοκόλλου.

\*\*\* *Ports* *49152-65535:* Θύρες που χρησιμοποιούνται από τους clients καθώς είναι unregistered.

**Ports:** - 22 Secure Shell (SSH),[11] secure logins, file transfers (scp, sftp) and port forwarding.

- 80/443 Hypertext Transfer Protocol (HTTP)[48][49] uses TCP in versions 1.x and 2.

- 53 Domain Name System(DNS).