Ασφάλεια Συστημάτων και Υπηρεσιών

Φθινόπωρο 2021

7η Άσκηση

Υποθέτουμε ότι ρυθμίζουμε το τείχος προστασίας (stateful firewall) του Πολυτεχνείου Κρήτης (εύρος IPv4 διευθύνσεων: 147.27/16).

Το τείχος προστασίας επιτρέπει στους εσωτερικούς χρήστες να περιηγούνται σε εξωτερικούς ιστοτόπους και να συνδέονται σε εξωτερικούς υπολογιστές με secure shell (ssh, sftp και οποιαδήποτε υπηρεσία υλοποιείται πάνω από ssh)

Το τείχος προστασίας επιτρέπει στους εξωτερικούς χρήστες να συνδέονται στον web server του Π.Κ (https://www.tuc.gr)

Το τείχος προστασίας επιτρέπει την αναζήτηση πληροφοριών DNS (Domain Name System) από και προς κάθε κατεύθυνση.

Το τείχος προστασίας δεν επιτρέπει πακέτα του πρωτοκόλλου ICMP προς τον web server του Π.Κ, ενώ αντιθέτως επιτρέπει πακέτα του πρωτοκόλλου ICMP από τους εσωτερικούς χρήστες προς οπουδήποτε εκτός του Π.Κ.

Επειδή πρόκειται για stateful firewall ελέγχει μέσω του Flag Bit αν η σύνδεση πρόκειται για νέα ή γίνεται κακόβουλη προσπάθεια με ειδικά διαμορφωμένα πακέτα TCP.

1. Συμπληρώστε τον πίνακα πολιτικών του τείχους προστασίας:

Action	Source Address	Dest address	Protocol	Source port	Dest port	Flag Bit	Check connection	Description
Allow/Reject/Deny	Internet/TUC	Internet/TUC	TCP/UDP					
……..								
…….								

Action: Μία από τις Allow, Reject, Deny

Source Address: Μία από Internet (περιλαμβάνει τις διευθύνσεις εκτός TUC), TUC (περιλαμβάνει τις διευθύνσεις 147.27/16)

Πρωτόκολλο: TCP ή UDP ή ICMP

Source Port: Πηγαία θύρα σύνδεσης

Dest Port: Θύρα προορισμού σύνδεσης

Flag Bit set: Τιμές ANY ή ACK ή SYN ή FIN ή RST ή SYNACK

Check Connection: Τιμή X αν έχει τεθεί κακόβουλα το Flag Bit

2. Σε περίπτωση που υλοποιούσατε το συγκεκριμένο τείχος προστασίας σε ένα Linux PC, ποιος θα ήταν ο ελάχιστος αριθμός καρτών Ethernet που θα έπρεπε να είχε το PC. Δικαιολογήστε σε μία γραμμή την απάντησή σας.

Παραδοτέα:

Μία τεχνική αναφορά σε pdf ανά άτομο με συμπληρωμένο τον πίνακα πολιτικών του τείχους προστασίας. Για κάθε πολιτική θα πρέπει να έχετε σαφή περιγραφή (πεδίο description του πίνακα): π.χ η πολιτική της γραμμής 1 αποτρέπει / επιτρέπει /απορρίπτει τα πακέτα του πρωτοκόλλου TCP που κατευθύνονται από «source address» σε «dest address» και αυτό γίνεται για να αποτραπεί / επιτραπεί / απορριφθεί η επικοινωνία με το πρωτόκολλο «xxx» μεταξύ «χρηστών Πολυτεχνείου Κρήτης» και «Internet». Μπορείτε για ευκολία να τοποθετήσετε την περιγραφή κάτω από τον πίνακα.

Υπόδειξη: Προσοχή στην διαφορά του πρωτοκόλλου ICMP έναντι των TCP/UDP και του UDP έναντι του TCP.

Σε κάθε περίπτωση περιοριστείτε στην στοίβα πρωτοκόλλων IPv4 και μην επεκταθείτε στην στοίβα πρωτοκόλλων IPv6

Η τεχνική αναφορά θα ονομαστεί ως <yourlastnameAM>_assign7, και θα την ανεβάσετε στο eclass π.χ christodoulou2018123456_assign7.pdf

Η αναφορά σας δεν πρέπει να υπερβαίνει την 1 σελίδα.

Βιβλιογραφία:

TCP

https://www.tutorialspoint.com/data_communication_computer_network/transmission_control_protocol.htm

UDP

https://www.techtarget.com/searchnetworking/definition/UDP-User-Datagram-Protocol

ICMP

https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

Well known ports

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers