Ασφάλεια Συστημάτων και Υπηρεσιών

Αναφορά $7^{ης}$ Άσκησης

Γιουμερτάκης Απόστολος, 2017030142

Άσκηση 1

Κατασκευή πίνακα πολιτικών του τείχους προστασίας

	Action	Source Address	Dest Address	Protocol	Source Port	Dest Port	Flag bit	Check connection	Description
1	Allow	Internet	TUC	TCP	ANY	80	ANY	0	HTTP in (server)
2	Allow	Internet	TUC	TCP	ANY	443	ANY	0	HTTPs in (server)
3	Allow	TUC	Internet	TCP	80	ANY	ANY	0	HTTP out (server)
4	Allow	TUC	Internet	TCP	443	ANY	ANY	0	HTTPs out (server)
5	Allow	Internet	TUC	TCP	80	ANY	ANY	0	HTTP in (client)
6	Allow	Internet	TUC	TCP	443	ANY	ANY	0	HTTPs in (client)
7	Allow	TUC	Internet	TCP	ANY	80	ANY	0	HTTP out (client)
8	Allow	TUC	Internet	TCP	ANY	443	ANY	0	HTTPs out (client)
9	Allow	Internet	TUC	TCP	22	ANY	ACK	1	SSH, SFTP in (client)
10	Allow	TUC	Internet	TCP	ANY	22	ACK	1	SSH, SFTP out (client)
11	Allow	TUC	Internet	UDP/ TCP	53	ANY	ACK	1	DNS server
12	Allow	Internet	TUC	UDP/ TCP	ANY	53	ANY	0	DNS server
13	Allow	TUC	Internet	UDP/ TCP	ANY	53	ANY	0	DNS external
14	Allow	Internet	TUC	UDP/ TCP	53	ANY	ACK	1	DNS external
15	Reject	Internet	TUC	ICMP	ANY	ANY	ANY	0	ICMP in
16	Allow	TUC	Internet	ICMP	ANY	ANY	ANY	0	ICMP out
17	Deny	0.0.0.0	0.0.0.0	TCP	ANY	ANY	ANY	–	NONE

Action:

- Allow: Επιτρέπει την πρόσβαση στα συγκεκριμένα ports.
- Allow: Απότρέπει την πρόσβαση στα συγκεκριμένα ports, χωρίς καμία απάντηση στον χρήστη (client).
- Reject: Απότρέπει την πρόσβαση στα συγκεκριμένα ports, στέλνοντας την απάντηση 'Destination is unreachable' στον χρήστη (client).

Κανόνας 1,2:
Επιτρέπει την αποστολή πακέτων από εξωτερικό υπολογιστή πρός το Πολυτεχνείο Κρήτης για πρωτόκολλα HTTP, HTTPs για πρόσβαση σε ιστοσελίδες όπως το tuc.gr, με όλα τα flags ενεργοποιημένα.

Κανόνας 3,4:
Επιτρέπει την αποστολή πακέτων (απαντήσεων) από servers του Πολυτεχνείου Κρήτης προς εξωτερικό υπολογιστή για πρωτόκολλα HTTP, HTTPs για πρόσβαση σε ιστοσελίδες όπως το tuc.gr, με όλα τα flags ενεργοποιημένα.

Κανόνας 5,6:
Επιτρέπει την αποστολή πακέτων από υπολογιστές του Πολυτεχνείου Κρήτης προς εξωτερικούς servers για πρωτόκολλα HTTP, HTTPs για πρόσβαση σε ιστοσελίδες όπως το google.com, με όλα τα flags ενεργοποιημένα.

Κανόνας 7,8:
Επιτρέπει την αποστολή πακέτων (απαντήσεων) από εξωτερικούς servers προς υπολογιστές του Πολυτεχνείου Κρήτης για πρωτόκολλα HTTP, HTTPs για πρόσβαση σε ιστοσελίδες όπως το google.com, με όλα τα flags ενεργοποιημένα.

Κανόνας 9:
Επιτρέπει την αποστολή πακέτων (απαντήσεων) από εξωτερικούς servers προς υπολογιστές του Πολυτεχνείου Κρήτης για πρόσβαση με secure shell (πρωτόκολλα SSH, SFTP και οποιαδήποτε υπηρεσία υλοποιείται πάνω από ssh).

Κανόνας 10:
Επιτρέπει την αποστολή πακέτων από υπολογιστές του Πολυτεχνείου Κρήτης προς εξωτερικούς servers για πρόσβαση με secure shell (πρωτόκολλα SSH, SFTP και οποιαδήποτε υπηρεσία υλοποιείται πάνω από ssh).

Κανόνας 11:
Επιτρέπει την αποστολή πακέτων (απαντήσεων) από τον server του Πολυτεχνείου Κρήτης προς εξωτερικούς υπολογιστές για αναζήτηση πληροφοριών DNS, με τα πρωτόκολλα UDP, TCP αντίστοιχα (το πρωτόκολλο UDP πιο διαδεδομένο από το TCP για εφαρμογές DNS). Το flag: ACK έχει νόημα μόνο όταν το πρωτόκολλο είναι TCP.

Κανόνας 12:
Επιτρέπει την λήψη πακέτων (queries) από εξωτερικούς υπολογιστές προς τον server του Πολυτεχνείου Κρήτης για αναζήτηση πληροφοριών DNS, με τα πρωτόκολλα UDP, TCP αντίστοιχα (το πρωτόκολλο UDP πιο διαδεδομένο από το TCP για εφαρμογές DNS).

Κανόνας 13:
Επιτρέπει την αποστολή πακέτων (queries) από υπολογιστές του Πολυτεχνείου Κρήτης προς εξωτερικούς servers για αναζήτηση πληροφοριών DNS, με τα πρωτόκολλα UDP, TCP αντίστοιχα.

Κανόνας 14:
Επιτρέπει την λήψη πακέτων (απαντήσεων) από εξωτερικούς servers προς υπολογιστές του Πολυτεχνείου Κρήτης για αναζήτηση πληροφοριών DNS, με τα πρωτόκολλα UDP, TCP αντίστοιχα. Το flag: ACK έχει νόημα μόνο όταν το πρωτόκολλο είναι TCP.

Κανόνας 15:
Απότρέπει την λήψη πακέτων από εξωτερικούς υπολογιστές προς webservers του Πολυτεχνείου Κρήτης για έλεγχο και διαχείρηση των συστημάτων, με το πρωτόκολλο ICMP.

Κανόνας 16:
Επιτρέπει την αποστολή πακέτων από υπολογιστές του Πολυτεχνείου Κρήτης προς εξωτερικούς servers για έλεγχο και διαχείρηση των συστημάτων, με το πρωτόκολλο ICMP.

Κανόνας 16:
Μπλοκάρεται όλη η κίνηση για οποιαδήποτε άλλη υπηρεσία ¨τρέχει' σε ports.

Άσκηση 2

Ερώτηση:
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.

Απάντηση:
Χρειάζονται τουλάχιστον δύο(2) κάρτες για την λειτουργία του τείχους προστασίας, μια με στατική τοπική διεύθυνση IP (147.27.x.x) και μια με εξωτερική διεύθυνση IP, ώστε να μπορεί να δει τις διευθύνσεις κάθε εσωτερικού αλλά και εξωτερικού υπολογιστή.

Τα παραπάνω επιβεβαιώθηκαν στο μέγιστο δυνατό χρησιμοποιώντας το πρόγραμμα καταγραφής πακέτων, Wireshark.