ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Εργασία με χρήση του λογισμικού WireShark

Διαδικαστικά

Η εργασία μπορεί να εκπονηθεί ατομικά ή σε ομάδα δύο ατόμων. Θα πρέπει να υποβάλλετε τις απαντήσεις σας (1 υποβολή ανά ομάδα) μέχρι τη **Δευτέρα 16 Ιανουαρίου 2023**, στις 23:55, μέσω του εργαλείου «Υποβολή Εργασιών» του e-class.

Το παραδοτέο της εργασίας θα είναι **ένα έγγραφο PDF**, το οποίο θα περιέχει τις απαντήσεις σας με σαφήνεια και περιεκτικότητα μαζί με κατάλληλα screenshots από το wireshark. Το παραδοτέο θα πρέπει να έχει ως όνομα τους αριθμούς μητρώου των φοιτητών που το ετοίμασαν, και _wireshark π.χ. 3200400_3200300_wireshark.pdf.

Αντικείμενο εργασίας

Η εργασία έχει στόχο τη χρήση του εργαλείου WireShark για συλλογή πακέτων από τοπικό δίκτυο και την ανάλυση της λειτουργίας δικτυακών πρωτοκόλλων. Για να εγκαταστήσετε το εργαλείο WireShark στον υπολογιστή σας θα πρέπει να το κατεβάσετε από τον ακόλουθο σύνδεσμο: https://www.wireshark.org/#download. Στην περιγραφή της εργασίας, θεωρούμε ότι δουλεύετε σε Windows (οι τροποποιήσεις για Linux και Mac OSX είναι ελάχιστες).

Μέρος Α’

ΟΔΗΓΙΕΣ

Το **traceroute** χρησιμοποιεί το πρωτόκολλο ICMP (Internet Control Message Protocol) για να ανακαλύψει τη διαδρομή που ακολουθεί ένα IP πακέτο από τον τοπικό host προς ένα απομακρυσμένο host.

1. Ξεκινήστε την εφαρμογή Wireshark.
2. Ανοίξτε ένα παράθυρο με **command prompt**.
3. Ξεκινήστε τη διαδικασία ανίχνευσης (capturing) πακέτων.
4. Στο command prompt παράθυρο δώστε την εντολή:
   `tracert www.ieee.org` (windows) ή **`traceroute www.ieee.org`** (linux, Mac OS)
   (Κρατήστε screenshot από την εκτέλεση της εντολής και συμπεριλάβετέ το στις απαντήσεις σας).
5. Σταματήστε την ανίχνευση πακέτων.
6. Απαντήστε στις ακόλουθες ερωτήσεις με βάση την πληροφορία που έχει κάνει capture το WireShark.

ΕΡΩΤΗΣΕΙΣ

1. Ποια ήταν η χρονική διάρκεια της ανίχνευσής σας;
2. Προσδιορίστε σε ένα πίνακα, ποια διαφορετικά πρωτόκολλα ανιχνεύθηκαν κατά τη χρονική διάρκεια της ανίχνευσης, διαχωρίζοντάς τα σύμφωνα με τα επίπεδα στα οποία ανήκουν.

3. Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.
4. Ποιο φίλτρο θα χρησιμοποιήσετε ώστε να εμφανίζονται στο παράθυρο του wireshark μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;
5. Εξετάστε το IP πακέτο που μεταφέρει το **πρώτο ICMP Echo Request**.
   a. Ποια είναι η IP διεύθυνση του destination;
   b. Πόσο είναι το time-to-live του πακέτου (ή το hop limit αν στο δίκτυο του provider τρέχει η IPv6 και όχι η IPv4 έκδοση του πρωτοκόλλου IP);
   c. Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;
6. Εξετάστε το IP πακέτο που μεταφέρει το **πρώτο ICMP Time Exceeded**.
   a. Ποια είναι η IP διεύθυνση του destination;
   b. Ποια είναι η IP διεύθυνση του source;
7. Αναφέρατε όλες τις source IP διευθύνσεις των πακέτων που μεταφέρουν ICMP Time Exceeded μηνύματα. Υπάρχει αντιστοιχία με αυτές που φαίνονται κατά την εκτέλεση της εντολής tracert στο command prompt παράθυρο;

Μέρος Β'

ΟΔΗΓΙΕΣ

1. Ανοίξτε ένα παράθυρο με **command prompt** στο λειτουργικό.
2. Με τη χρήση της εντολής **ipconfig /flushdns**, καθαρίστε την προσωρινή μνήμη (cache) DNS του υπολογιστή σας, έτσι ώστε στα παρακάτω να χρειάζεται επικοινωνία με DNS Server.
3. Ξεκινήστε τη διαδικασία ανίχνευσης (**capturing**) πακέτων.
4. Κατά τη διάρκεια της ανίχνευσης ανοίξτε τον **browser** που χρησιμοποιείτε για την πλοήγηση στο WWW. Επισκεφθείτε τον Ιστότοπο **http://www.openoffice.org/.**
5. Σταματήστε τη διαδικασία ανίχνευσης.
6. Απαντήστε στις ακόλουθες ερωτήσεις με βάση την πληροφορία που έχει κάνει capture το WireShark.

ΕΡΩΤΗΣΕΙΣ

1. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;
2. Πόσα και ποια είναι τα διαφορετικά endpoints (η σχετική πληροφορία βρίσκεται στο μενού Statistics) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Μπορείτε να βρείτε σε τί είδους συσκευές αντιστοιχούν;
3. Πόσα είναι τα διαφορετικά endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα endpoints σε επίπεδο Ethernet; Αν όχι, εξηγείστε γιατί συμβαίνει αυτό.
4. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν για την ερώτηση από τον υπολογιστή σας προς τον DNS server και για την απάντηση του DNS server.
5. Πώς διακρίνετε αν ένα πακέτο περιέχει αίτημα προς τον DNS server ή απάντηση σε ερώτημα που έχετε κάνει; Πώς συνδέονται το πακέτο μιας απάντησης με το πακέτο της ερώτησης;
6. Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει είναι authoritative για το συγκεκριμένο domain; Ο name server που μας έχει απαντήσει είναι authoritative για το συγκεκριμένο domain;
7. Το όνομα **www.openoffice.org** είναι κανονικό dns όνομα ή alias; Ποια είναι η IP διεύθυνση που του αντιστοιχεί;
8. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το **www.openoffice.org** υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων. Δώστε ένα screenshot από το Wireshark που να περιέχει τα segments αυτά. Εξηγήστε τη

διαδικασία χειραψίας τριών βημάτων με βάση την πληροφορία που περιέχεται στα TCP segments αυτά.

9. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το TCP πρωτόκολλο για την επικοινωνία με τον server που φιλοξενεί το **www.openoffice.org.**
10. Μπορείτε να δείτε τα πακέτα που περιέχουν HTTP GET αίτημα από τον Browser σας προς τον Web Server; Αν ναι, προς ποιες IP διευθύνσεις στάλθηκαν. Αν όχι, εξηγείστε γιατί.