ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
SCHOOL OF INFORMATION SCIENCES & TECHNOLOGY

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
DEPARTMENT OF INFORMATICS

ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

1η Εργασία με χρήση του λογισμικού WireShark

Διαδικαστικά

Η εργασία αυτή είναι ατομική. Θα πρέπει να υποβάλλετε τις απαντήσεις σας μέχρι την **Τετάρτη 25 Νοεμβρίου 2020**, στις 23:55, μέσω του εργαλείου «Υποβολή Εργασιών» του e-class.

Το παραδοτέο της εργασίας θα είναι **ένα έγγραφο PDF**, στο οποίο θα περιγράφετε με σαφήνεια και περιεκτικότητα τη διαδικασία που ακολουθήσατε μαζί με κατάλληλα screenshots. Το παραδοτέο θα πρέπει να έχει ως όνομα τον αριθμό μητρώου του/της φοιτητή/τριας που το ετοίμασε, και _wireshark_1 π.χ. 3180400_wireshark_1.pdf.

Αντικείμενο εργασίας

Η εργασία έχει στόχο τη χρήση του εργαλείου WireShark για συλλογή πακέτων από τοπικό δίκτυο και την ανάλυση της λειτουργίας του Πρωτοκόλλου ICMP. 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).

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.acm.org` (windows) ή **`traceroute www.acm.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;