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

2η Εργασία με χρήση του λογισμικού WireShark

Διαδικαστικά

Η εργασία αυτή είναι ατομική. Θα πρέπει να υποβάλλετε τις απαντήσεις σας μέχρι την **Παρασκευή 15 Ιανουαρίου 2021**, στις 23:55, μέσω του εργαλείου «Εργασίες» 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_2 π.χ. 3180400_wireshark_2.pdf.

Αντικείμενο εργασίας

Η εργασία έχει στόχο τη χρήση του εργαλείου WireShark για τη μελέτη του Συστήματος Ονοματοδοσίας Περιοχής (**Domain Name System**) σε συνδυασμό με τη χρήση του πρωτοκόλλου **HTTP** για την περιήγηση στο WWW.

Το Internet χρησιμοποιεί ένα κατανεμημένο σύστημα ονοματοδοσίας που ονομάζεται Domain Naming System (DNS). Το σύστημα DNS μας επιτρέπει να αναφερόμαστε σε υπολογιστές και άλλες συσκευές με ονόματα (συστημάτων ή host names) και όχι με την IP διεύθυνση, η οποία είναι δύσκολη μνημονικά και άβολη στην χρήση. Για παράδειγμα, είναι πιο εύκολο να θυμόμαστε το www.aueb.gr παρά το 195.251.255.156. Το DNS είναι υπεύθυνο να αντιστοιχίζει τα μνημονικά ονόματα (host names) με τις σχετικές IP διευθύνσεις. Ο υπολογιστής μας προκειμένου να ανακαλύψει ποια IP διεύθυνση αντιστοιχεί σε κάποιο όνομα (ή URL) το οποίο του δίνουμε για να επικοινωνήσει, ελέγχει πρώτα στην τοπική του cache και αν δεν βρει εκεί την απάντηση, ρωτάει τον **name server** του domain στο οποίο ανήκει (ο υπολογιστής μας). Στην περιγραφή της εργασίας, θεωρούμε ότι δουλεύετε σε Windows (οι τροποποιήσεις για Linux και Mac OSX είναι ελάχιστες).

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.book4book.gr/.**
5. Σταματήστε τη διαδικασία ανίχνευσης.

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 ποιες συσκευές αντιστοιχούν;
3. Πόσα και ποια 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.book4book.gr είναι domain ή canonical name; Ποια είναι η IP διεύθυνση που αντιστοιχεί στο www.book4book.gr;
8. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το www.book4book.gr 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 HTTP πρωτόκολλο. Ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιεί το HTTP;
10. Πόσα πακέτα που περιείχαν HTTP GET αίτημα έστειλε ο browser σας; Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;
11. Ποια έκδοση του HTTP τρέχει ο browser σας; Ποια έκδοση τρέχει ο server; Ποιο λογισμικό web server «τρέχει» ο server που σας απάντησε για το site www.book4book.gr;