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

Εργασία με χρήση του λογισμικού WireShark

Διαδικαστικά

Η εργασία αυτή είναι ατομική. Θα πρέπει να υποβάλλετε τις απαντήσεις σας μέχρι την **Πέμπτη 10 Ιανουαρίου 2019**, 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 π.χ. 3160400.pdf.

Αντικείμενο εργασίας

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

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. Στο command prompt παράθυρο δώστε την εντολή:
   `ipconfig /flushdns`
   Έτσι ώστε να καθαρίστε την προσωρινή μνήμη DNS του υπολογιστή σας και στη συνέχεια να χρειάζεται επικοινωνία με DNS Server.
4. Ξεκινήστε τη διαδικασία ανίχνευσης (capturing) πακέτων.
5. Στο command prompt παράθυρο δώστε την εντολή:
   `tracert www.iana.org`

(Κρατήστε screenshot από την εκτέλεση της εντολής και συμπεριλάβετέ το στις απαντήσεις σας).

6. Σταματήστε την ανίχνευση πακέτων.
7. Απαντήστε στις ακόλουθες ερωτήσεις με βάση την πληροφορία που έχει ανιχνεύσει το WireShark.

Γενικές Ερωτήσεις

1. Ποια ήταν η χρονική διάρκεια της ανίχνευσής σας;
2. Προσδιορίστε σε ένα πίνακα, ποια διαφορετικά πρωτόκολλα χρησιμοποίησε ο υπολογιστής σας στη 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. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;
5. 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;
6. 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.

Ερωτήσεις σχετικά με το DNS

7. 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.
8. 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;
9. Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει για το www.iana.org είναι authoritative για το συγκεκριμένο domain; Είναι ο name server που μας έχει απαντήσει authoritative για το συγκεκριμένο domain;
10. Το όνομα www.iana.org είναι domain name ή πρόκειται για canonical name;
11. Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.iana.org; Ποια είναι η IP διεύθυνση του δικού σας υπολογιστή;

Ερωτήσεις σχετικά με το ICMP

12. Πως θα δείτε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;
13. 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;
    c. Πόσο είναι το μέγεθος (length) των δεδομένων που μεταφέρει;

14. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Time Exceeded.
    a. Ποια είναι η IP διεύθυνση του destination; Ποια είναι η IP διεύθυνση του Source;
15. Ελέγχοντας το time-to-live των διαδοχικών πακέτων ICMP Echo Request, τί παρατηρείτε; Για ποιο λόγο γίνεται αυτό;
16. Υπολογίστε το χρόνο ανάμεσα στο $1^{ο}$ ICMP Echo Request και το αντίστοιχο ($1^{ο}$) ICMP Time Exceeded και συγκρίνετέ τον με τους χρόνους που δίνει αντίστοιχα το πρώτο βήμα της εκτέλεσης της εντολής tracert στο command prompt παράθυρο.
17. 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;

Ανοίξτε ένα παράθυρο με **command prompt** στο λειτουργικό. Με τη χρήση της εντολής **ipconfig /flushdns**, καθαρίστε την προσωρινή μνήμη DNS του υπολογιστή σας, έτσι ώστε στα παρακάτω να χρειάζεται επικοινωνία με DNS Server. Ξεκινήστε τη διαδικασία ανίχνευσης (**capturing**) πακέτων. Κατά τη διάρκεια της ανίχνευσης ανοίξτε τον **browser** που χρησιμοποιείτε για την πλοήγηση στο WWW. Πληκτρολογήστε το URL **http://www.lib.aueb.gr/** για να πλοηγηθείτε στον ιστότοπο της βιβλιοθήκης του Πανεπιστημίου ή εναλλακτικά το URL **http://eudoxus.gr/**. Σταματήστε τη διαδικασία ανίχνευσης.

Ερωτήσεις

1. Προσδιορίστε σε ένα πίνακα, ποια διαφορετικά πρωτόκολλα χρησιμοποίησε ο υπολογιστής σας στη χρονική διάρκεια της ανίχνευσης, διαχωρίζοντάς τα σύμφωνα με τα επίπεδα στα οποία ανήκουν.
2. Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.
3. Πόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν;
4. 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;
5. 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.
6. 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.
7. 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;
8. 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;
9. Το όνομα www.lib.aueb.gr (ή αντίστοιχα το eudoxus.gr) αντιστοιχίζεται με IP διεύθυνση ή πρόκειται για canonical name;
10. Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.lib.aueb.gr (ή αντίστοιχα στο eudoxus.gr); Ποια η IP διεύθυνση του δικού σας υπολογιστή;
11. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το www.lib.aueb.gr (eudoxus.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.
12. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο.
13. Πόσα πακέτα που περιείχαν HTTP GET αίτημα έστειλε ο browser σας; Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;

14. Ποια έκδοση του HTTP τρέχει ο browser σας; Ποια έκδοση τρέχει ο server;
15. Ποιες γλώσσες υποδεικνύει ο browser στον server ότι μπορεί να δεχθεί;