ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Εργασία με χρήση του λογισμικού WireShark

Διαδικαστικά

Η εργασία αυτή είναι **ατομική**. Θα πρέπει να υποβάλλετε τις απαντήσεις σας μέχρι την **Τετάρτη 15 Ιανουαρίου 2025**, 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 τον αριθμό μητρώου του/της φοιτητή/τριας που το ετοίμασε π.χ. 3220400.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).

Άσκηση 1 - ICMP

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. *Σημείωση: αν το δίκτυό σας τρέχει σε IPv6 (128bits IP addresses), τότε θα τρέχει το πρωτόκολλο ICMPv6.*

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.github.com (windows) ή **traceroute www.github.com** (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 (*όπως τα εμφανίζει το wireshark*).
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. Ποιες είναι οι συσκευές που επικοινωνούν σε επίπεδο Ethernet; Ποιες είναι οι MAC διευθύνσεις τους;
   b. Ποια είναι η IP διεύθυνση του υπολογιστή σας;
   c. Ποια είναι η IP διεύθυνση του destination;
   d. 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*);
   e. 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;

Άσκηση 2 – DNS & HTTP

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.
5. Επισκεφθείτε τον Ιστότοπο **http://www.faqs.org.**
6. Επισκεφθείτε τον Ιστότοπο **https://www.aueb.gr**.
7. Σταματήστε τη διαδικασία ανίχνευσης.
8. 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. 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;
5. Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει είναι **authoritative** για το συγκεκριμένο domain; Ο name server που έχει απαντήσει είναι authoritative για το συγκεκριμένο domain;

6. Το όνομα **www.faqs.org** είναι κανονικό dns όνομα ή alias; Ποια είναι η IP διεύθυνση που του αντιστοιχεί;
7. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το **www.faqs.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.
8. 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.faqs.org.**
9. 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.
10. Βρείτε το πρώτο **HTTP GET** μήνυμα του υπολογιστή σας προς τον server που φιλοξενεί το **www.faqs.org**.
    a. Ποια έκδοση του HTTP χρησιμοποιεί ο browser σας;
    b. Η σύνδεση είναι persistent ή non-persistent; Πως το συμπεραίνετε;
11. Εντοπίστε το μήνυμα με το οποίο απαντάει στο HTTP GET αυτό ο web server.
    a. Ποια έκδοση του HTTP χρησιμοποιεί ο server;
    b. Ποιο είναι το λογισμικό που υλοποιεί τον web server;
    c. Ποιο είναι το μέγεθος και ο τύπος του αρχείου που στέλνει πίσω ο web server;
12. Ποιο είναι το **πρώτο frame** που ανταλλάσσεται μεταξύ του υπολογιστή σας και του server που φιλοξενεί το **www.aueb.gr**; Ποια η λειτουργία του frame αυτού;
13. Σε ποιο port δέχεται αιτήματα πελατών ο server για το site **www.aueb.gr**;
14. Μπορείτε να δείτε το περιεχόμενο των HTTP μηνυμάτων που ανταλλάσσει ο υπολογιστής σας με τον web server που φιλοξενεί το **www.aueb.gr**; Εξηγείστε την απάντησή σας.
15. Ποια έκδοση του **Transport Layer Security** πρωτοκόλλου χρησιμοποιούν στη μεταξύ τους επικοινωνία ο υπολογιστής σας με το www.aueb.gr;