ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ

ΕΡΓΑΣΙΑ ΜΕ ΧΡΗΣΗ ΤΟΥ ΕΡΓΑΛΕΙΟΥ WIRESHARK

(Ακαδημαϊκό έτος 2022-2023)

Διαδικαστικά

Η εργασία είναι ατομική. Θα πρέπει να υποβάλετε τις απαντήσεις σας μέχρι τις **15 Ιανουαρίου 2023**, μέσω του εργαλείου «Υποβολή Εργασιών» του e-class. Οι απαντήσεις σας θα πρέπει να περιέχονται σε ένα έγγραφο σε μορφή PDF, τεκμηριωμένες με περιγραφή της διαδικασίας που ακολουθήσατε, συνοδευόμενη από κατάλληλα screenshots.

Γενικά

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. Στις παρακάτω ασκήσεις, θεωρούμε ότι έχετε ήδη ξεκινήσει την εφαρμογή, και ότι δουλεύετε σε Windows (οι τροποποιήσεις για Linux και Mac OSX είναι ελάχιστες).

Άσκηση 1

- 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.
- Επιλέξτε το **interface** με το οποίο συνδέεστε στο δίκτυο και *ξεκινήστε* στο Wireshark τη διαδικασία **capture**.
- Αφήστε το εργαλείο να συλλέξει για 1-2 λεπτά τα πακέτα που στέλνονται/λαμβάνονται από τον υπολογιστή σας καθώς τον χρησιμοποιείτε για πλοήγηση στο WWW ή άλλες δραστηριότητες που απαιτούν επικοινωνία με το δίκτυο. Μεταξύ των sites που θα επισκεφθείτε να είναι και ο Ιστότοπος **http://www.faqs.org/**.
- Σταματήστε τη διαδικασία **capture**.

Απαντήστε στα παρακάτω ερωτήματα, παραθέτοντας και τα σχετικά screenshots με τις απαντήσεις, όπως εμφανίζονται στο εργαλείο:

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. Ποιο **πρωτόκολλο επιπέδου μεταφοράς** χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.

2. Πόσα και ποια είναι τα διαφορετικά **endpoints** (η σχετική πληροφορία βρίσκεται στο μενού *Statistics*) με τα οποία υπάρχει επικοινωνία σε επίπεδο Ethernet; Πόσα και ποια είναι τα διαφορετικά **endpoints** με τα οποία υπάρχει επικοινωνία σε επίπεδο IP; Ταυτίζονται με τα **endpoints** σε επίπεδο Ethernet; Εξηγείστε γιατί.
3. Πόσα πακέτα **TCP** και πόσα πακέτα **UDP** στάλθηκαν;
4. 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.
5. Πόσα πακέτα **TCP** είχαν ως **destination port την 443** και πόσα την είχαν ως **source port**;
6. Πόσα πακέτα **TCP** είχαν ως **destination port την 80** και πόσα την είχαν ως **source port**;
7. 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**.
8. Πόσα πακέτα περιείχαν δεδομένα για το πρωτόκολλο **Transport Layer Security** (tls); Για ποιο Application Protocol «μεταφέρει δεδομένα» το TLS;
9. Πόσα πακέτα μετέφεραν δεδομένα **HTTP**;
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.
11. Ποιο λογισμικό web server «τρέχει» στο μηχάνημα που φιλοξενεί το **www.faqs.org;** Η σύνδεση μεταξύ web browser και του web server που φιλοξενεί το **www.faqs.org**, είναι persistent ή non-persistent;
12. Απομονώστε όλα τα πακέτα που χρησιμοποιούνται από το **DNS** εφαρμόζοντας το κατάλληλο φίλτρο.
13. 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;
14. Το **www.faqs.org** είναι dns name ή alias; Ποια είναι η IP διεύθυνση που του αντιστοιχεί;
15. 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;

Άσκηση 2

- Ανοίξτε ένα παράθυρο **command prompt**. Με τη χρήση της εντολής **ipconfig /release**, απελευθερώστε την IP διεύθυνση που έχει δοθεί στον υπολογιστή σας από το DHCP server, έτσι ώστε η IP διεύθυνση του υπολογιστή σας να γίνει 0.0.0.0.
- Ξεκινήστε τη διαδικασία ανίχνευσης (capturing) πακέτων.

- Στο command prompt παράθυρο, δώστε την εντολή: **ipconfig /renew.** Με την εντολή αυτή, ο υπολογιστής σας θα πρέπει να ζητήσει νέες δικτυακές ρυθμίσεις από τον DHCP server.
- Δώστε εκ νέου την εντολή: **ipconfig /renew**.
- Δώστε πάλι την εντολή: **ipconfig /release.**
- Δώστε εκ νέου την εντολή: **ipconfig /renew.**
- Σταματήστε τη διαδικασία ανίχνευσης.

Απαντήστε στα παρακάτω ερωτήματα, παραθέτοντας και τα σχετικά screenshots με τις απαντήσεις, όπως εμφανίζονται στο εργαλείο:

1. Τα **DHCP μηνύματα** στέλνονται πάνω από TCP ή UDP;
2. Σχεδιάστε ένα χρονικό διάγραμμα, στο οποίο θα φαίνεται η **αλληλουχία** της πρώτης ανταλλαγής των 4 DHCP πακέτων Discover/Offer/Request/ACK μεταξύ πελάτη-εξυπηρετητή. Για κάθε πακέτο, θα πρέπει να φαίνονται τα port numbers πηγής και προορισμού.
3. Ποια είναι η **MAC** (link layer) διεύθυνση του υπολογιστή σας;
4. Ποιες τιμές στο **DCHP discover** μήνυμα διαφοροποιούν το μήνυμα από το DHCP request μήνυμα;
5. Ποια είναι η τιμή του **Transaction-ID** σε κάθε ένα από τα 4 πρώτα (Discover/Offer/Request/ACK) DHCP μηνύματα; Ποιες είναι οι τιμές των Transaction-ID στη 2η ομάδα (Request/ACK) DHCP μηνυμάτων; Ποιος ο σκοπός ύπαρξης του πεδίου Transaction-ID;
6. Ποια είναι η **IP διεύθυνση του DHCP server** σας;
7. Ποια **IP διεύθυνση προσφέρει** ο DHCP server στον υπολογιστή σας; Σε ποιο μήνυμα συμβαίνει αυτό;
8. Εξηγείστε το **λόγο ύπαρξης** της πληροφορίας σχετικά με τον router και το network mask μέσα στο DHCP Offer μήνυμα.
9. Εξηγείστε το λόγο ύπαρξης του πεδίου **lease time**. Ποιο είναι το lease time για την IP διεύθυνση που σας δόθηκε;
10. Κατά τη διάρκεια της ανταλλαγής των DHCP μηνυμάτων, έχουν σταλεί ή ληφθεί **ARP πακέτα**; Αν ναι, εξηγείστε γιατί στάλθηκαν αυτά τα πακέτα.