ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ

ΕΡΓΑΣΙΑ ΜΕ ΧΡΗΣΗ ΤΟΥ ΕΡΓΑΛΕΙΟΥ WIRESHARK

Υπεύθυνη Εργασίας: Άννα Κεφάλα

(Ακαδημαϊκό έτος 2023-2024)

Διαδικαστικά

Η εργασία είναι **ατομική**. Θα πρέπει να υποβάλετε τις απαντήσεις σας μέχρι τις **19 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://faqs.org/**.
- Σταματήστε τη διαδικασία **capture**.

Απαντήστε στα παρακάτω ερωτήματα, παραθέτοντας και τα σχετικά screenshots με τις απαντήσεις, όπως εμφανίζονται στο εργαλείο ή αναφέροντας τα φίλτρα που χρησιμοποιήσατε για να εντοπίσετε συγκεκριμένα πακέτα:

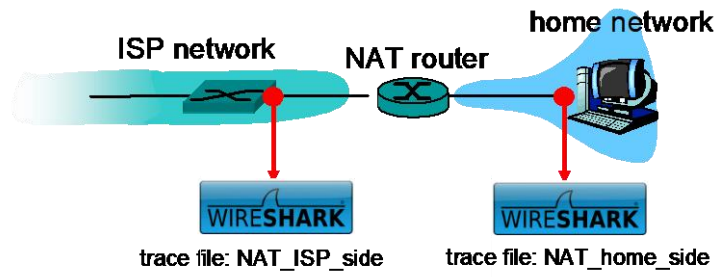
1. Προσδιορίστε σε ένα πίνακα, ποια διαφορετικά **πρωτόκολλα** χρησιμοποίησε ο υπολογιστής σας στη χρονική διάρκεια της ιχνηλάτησης, διαχωρίζοντάς τα σύμφωνα με τα επίπεδα στα

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. Πόσα πακέτα **TCP** είχαν ως **destination port την 443** και πόσα την είχαν ως **source port**;
5. Πόσα πακέτα **TCP** είχαν ως **destination port την 80** και πόσα την είχαν ως **source port**;
6. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το πρωτόκολλο **TCP** για την επικοινωνία με τον server που φιλοξενεί το **www.faqs.org**.
7. Πόσα πακέτα περιείχαν δεδομένα για το πρωτόκολλο **Transport Layer Security** (TLS); Για ποιο Application Protocol «μεταφέρει δεδομένα» το TLS;
8. Πόσα πακέτα μετέφεραν δεδομένα **HTTP**;
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. 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;
11. Απομονώστε όλα τα πακέτα που χρησιμοποιούνται από το **DNS** εφαρμόζοντας το κατάλληλο φίλτρο.
12. 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;
13. Το **www.faqs.org** είναι dns name ή alias; Ποια είναι η IP διεύθυνση που του αντιστοιχεί;
14. 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

Στόχος της άσκησης είναι να διερευνήσουμε τη χρήση του **πρωτοκόλλου NAT**. Μας ενδιαφέρει να δούμε τα πακέτα που συλλαμβάνονται (captured) όταν κάνουμε ένα απλό αίτημα HTTP από έναν υπολογιστή σε ένα οικιακό δίκτυο σε έναν δημόσιο web server (www.google.com). Στο οικιακό δίκτυο, ο δρομολογητής παρέχει υπηρεσία NAT. Στη διπλανή εικόνα φαίνεται το σενάριο το οποίο θα μελετήσουμε με το WireShark.



Δίνεται ένα αρχείο ιχνηλάτησης (trace file) "**NAT_home_side**" με τα πακέτα που έχουν γίνει captured στον web client στο εσωτερικό μας δίκτυο και ένα αρχείο ιχνηλάτησης "**NAT_ISP_side**" από τη σύνδεση του οικιακού δρομολογητή στο δίκτυο του ISP.

Ανοίξτε το αρχείο **NAT_home_side** και απαντήστε στις παρακάτω ερωτήσεις.

1. Ποια είναι η IP διεύθυνση του πελάτη;
2. Ο πελάτης στην πράξη επικοινωνεί με πολλούς διαφορετικούς διακομιστές της Google προκειμένου να εφαρμόσει την "ασφαλή περιήγηση" (safe browsing). Ο κύριος διακομιστής Google που θα εξυπηρετεί την κύρια ιστοσελίδα της Google έχει IP διεύθυνση 64.233.169.104. Τί **φίλτρο** μπορείτε να χρησιμοποιήσετε προκειμένου να εμφανίζονται μόνο τα πλαίσια που περιέχουν μηνύματα **HTTP** που αποστέλλονται **προς/από αυτόν τον διακομιστή Google**;
3. Ποιο είναι το πρώτο **HTTP GET** που αποστέλλεται από τον πελάτη στον διακομιστή Google (με διεύθυνση IP 64.233.169.104); Ποιες είναι οι IP διευθύνσεις προέλευσης και προορισμού και οι TCP θύρες προέλευσης και προορισμού στο IP datagram που μεταφέρει αυτό το HTTP GET;
4. Πότε λαμβάνεται το αντίστοιχο μήνυμα **HTTP 200 OK** από τον διακομιστή Google; Ποιες είναι οι IP διευθύνσεις προέλευσης και προορισμού και οι TCP θύρες προέλευσης και προορισμού στο IP datagram που μεταφέρει αυτό το μήνυμα HTTP 200 OK;
5. Προκειμένου να σταλεί μια εντολή GET σε έναν διακομιστή HTTP, το TCP πρέπει πρώτα να εγκαθιδρύσει **σύνδεση** χρησιμοποιώντας την **τριπλή χειραψία**.
    a. Πότε αποστέλλεται το TCP SYN segment από τον πελάτη προς το διακομιστή (με IP διεύθυνση 64.233.169.104) για την εγκαθίδρυση της σύνδεσης που χρησιμοποιείται για το 1ο GET;
    b. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του πελάτη και του διακομιστή Google, υλοποιούν την εγκαθίδρυση της σύνδεσης με τη χειραψία 3 βημάτων. Δώστε ένα screenshot από το Wireshark που να περιέχει τα segments αυτά.
    c. Ποιες είναι οι IP διευθύνσεις προέλευσης και προορισμού και οι TCP θύρες προέλευσης και προορισμού για το SYN segment; Ποιες είναι οι IP διευθύνσεις

προέλευσης και προορισμού και οι θύρες προέλευσης και προορισμού του ACK που αποστέλεται ως απάντηση στο SYN; Πότε λαμβάνεται αυτό το ACK στον πελάτη; (***Σημείωση****: για να βρείτε αυτά τα segments θα χρειαστεί να διαγράψετε την έκφραση φίλτρου που εισαγάγατε παραπάνω*).

Στη συνέχεια θα επικεντρωθούμε στα δύο μηνύματα HTTP (GET και 200 OK) και στα TCP segments SYN και ACK που προσδιορίστηκαν παραπάνω. Ο στόχος θα είναι να εντοπίσουμε αυτά τα δύο μηνύματα HTTP και δύο TCP segments στο αρχείο ιχνηλάτησης (NAT_ISP_side) που καταγράφει τη σύνδεση μεταξύ του δρομολογητή και του ISP.

Ανοίξτε το αρχείο **NAT_ISP_side**.

6. Στο αρχείο ιχνηλάτησης NAT_ISP_side, βρείτε το πρώτο μήνυμα **HTTP GET** που στάλθηκε από τον πελάτη στον διακομιστή Google με IP διεύθυνση 64.233.169.104. Ποιες είναι οι IP διευθύνσεις προέλευσης και προορισμού και οι TCP θύρες προέλευσης και προορισμού στο IP datagram που φέρει αυτό το HTTP GET (όπως καταγράφεται στο αρχείο NAT_ISP_side); Ποια από αυτά τα πεδία είναι τα ίδια και ποια είναι διαφορετικά από την απάντησή σας στην ερώτηση 3 παραπάνω;
7. Έχουν αλλάξει κάποια πεδία στο μήνυμα HTTP GET; Ποια από τα ακόλουθα πεδία στο IP datagram που φέρει το HTTP GET αλλάζουν: Version, Header Length, Flags, Checksum. Εάν κάποιο από αυτά τα πεδία έχει αλλάξει, εξηγήστε (με μία πρόταση) γιατί αυτό το πεδίο έπρεπε να αλλάξει.
8. Στο αρχείο ιχνηλάτησης NAT_ISP_side, βρείτε το πρώτο μήνυμα **HTTP 200 OK** από τον διακομιστή Google με IP διεύθυνση 64.233.169.104. Ποιες είναι οι IP διευθύνσεις προέλευσης και προορισμού και οι TCP θύρες προέλευσης και προορισμού στο IP datagram που μεταφέρει αυτό το μήνυμα HTTP 200 OK; Ποια από αυτά τα πεδία είναι τα ίδια και ποια είναι διαφορετικά από την απάντησή σας στην ερώτηση 4 παραπάνω;
9. Στο αρχείο ιχνηλάτησης NAT_ISP_side, σε ποια χρονική στιγμή καταγράφηκαν το TCP SYN segment από πελάτη σε διακομιστή και το TCP ACK segment από διακομιστή σε πελάτη που αντιστοιχεί στα τμήματα της ερώτησης 5 παραπάνω; Ποιες είναι οι IP διευθύνσεις προέλευσης και προορισμού και οι θύρες προέλευσης και προορισμού για αυτά τα δύο segments; Ποια από αυτά τα πεδία είναι τα ίδια και ποια είναι διαφορετικά από την απάντησή σας στην ερώτηση 5 παραπάνω;
10. Με βάση τις απαντήσεις σας στα παραπάνω ερωτήματα, ποιες καταχωρήσεις θα κάνατε στον **NAT translation table** όσον αφορά την HTTP επικοινωνία που εξετάσατε;