Λυδία Αθανασίου p3170003

ΕΡΓΑΣΙΑ ΔΙΚΤΥΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Α’ ΜΕΡΟΣ

Εισαγωγικά:

3) Αποτέλεσμα εντολής ipconfig /flushdns στο command prompt έτσι ώστε να καθαριστεί η προσωρινή μνήμη DNS του υπολογιστή και στη συνέχεια να χρειάζεται επικοινωνία με DNS Server.

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματα

5) Αποτέλεσμα εντολής tracert www.ieee.org στο command prompt

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματα

Γενικές Ερωτήσεις:

1. Η χρονική διάρκεια της ανίχνευσής ήταν 67.244231 msec
2. Πίνακας με τα διαφορετικά πρωτόκολλα που χρησιμοποίησε ο υπολογιστής στη χρονική διάρκεια της ανίχνευσης, διαχωρισμένα σύμφωνα με τα επίπεδα στα οποία ανήκουν.

|  |  |
| --- | --- |
| Πακέτο | Επίπεδο που ανήκει |
| TCP | Transfer layer |
| ICMP | Internet layer |
| ARP | Network access layer |
| DNS |  |
| HTTP |  |
| Hypertext transfer protocol HTTP | Application Layer |
| NBNS |  |
| TLSv1.2 |  |

1. Εξετάστε ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιούν τα πρωτόκολλα του επιπέδου εφαρμογής που έχετε εντοπίσει.

* Το πρωτόκολλο επιπέδου εφαρμογής DNS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
* Το πρωτόκολλο επιπέδου εφαρμογής HTTP χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: ICMP
* Το πρωτόκολλο επιπέδου εφαρμογής Hypertext transfer protocol HTTP χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
* Το πρωτόκολλο επιπέδου εφαρμογής NBNS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: UDP
* Το πρωτόκολλο επιπέδου εφαρμογής TLS χρησιμοποιεί το πρωτόκολλο επιπέδου μεταφοράς: TCP

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματα Με βοήθησε να τα εντοπίσω το παράθυρο του wireshark: statistics>protocol Hierarchy statistics

1. Εικόνα που περιέχει στιγμιότυπο οθόνης

   Περιγραφή που δημιουργήθηκε αυτόματαΠόσα πακέτα TCP και πόσα πακέτα UDP στάλθηκαν; Εφαρμόζοντας στο wireshark τα κατάλληλα φίλτρα και βλέποντας κάτω δεξιά το display/packets βλέπουμε ότι τα UDP πακέτα που στάλθηκαν είναι 85 ενώ τα TCP πακέτα που στάλθηκαν είναι 85.
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;

Τα endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο ethernet είναι 2 και φαίνονται στο παρακάτω screen. Τα endpoints αυτά αντιστοιχούν στις ακόλουθες συσκευές: τον υπολογιστή μου και το Wi-Fi (τρέχουμε στο command prompt την εντολή ipconfig).

Εικόνα που περιέχει άτομο

Περιγραφή που δημιουργήθηκε αυτόματαΕικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματα

1. 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.

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματαΤα endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP είναι 24 και φαίνονται στο παρακάτω screen. Τα endpoints αυτά δεν ταυτίζονται με τα endpoints σε επίπεδο ethernet. Αυτό συμβαίνει διότι τα endpoints ethernet είναι φυσικές διευθύνσεις που συνδέονται με κάρτα ασύρματης διασύνδεσης, κάρα διασύνδεσης ethernet ή ειδική διεύθυνση MAC για broadcast(η οποία προορίζεται να ληφθεί από όλους). Τα endpoints IP είναι λογικές διευθύνσεις, στο επίπεδο δικτύου, που χρησιμοποιούνται από συσκευές που έχουν διευθύνσεις IP σε κάθε τμήμα (επίσης αποκαλούμενες VLAN) του δικτύου. Θα χρησιμοποιήσετε τα στατιστικά στοιχεία του τελικού σημείου Ethernet αν θέλουμε να δούμε τι συμβαίνει στην κάρτα διασύνδεσης (κάρτα ethernet ή wifi) ή στους δρομολογητές που είναι ο επόμενος host σε εμάς ενώ το τελικό σημείο IP, εάν θέλουμε να δούμε όλα τα δεδομένα που αναφέρονται σε μια συγκεκριμένη διεύθυνση IP με την οποία επικοινωνούμε (οποιαδήποτε συσκευή στο τοπικό δίκτυο ή στο διαδίκτυο). Άρα πρόκειται για τελείως διαφορετικά πράγματα γι’ αυτό τα endpoints τους δεν ταυτίζονται.

Ερωτήσεις σχετικά με το DNS:

1. 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.

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματα

1. 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;

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματαΤο πακέτο μια απάντησης με το πακέτο της ερώτησης συνδέονται με το transaction ID . Οι αιτήσεις έχουν το ίδιο Id Με τις αντίστοιχες απαντήσεις τους.

1. Υπάρχει κάποια σημαία (flag) που να προσδιορίζει αν ο name server που μας απαντάει για το www.ieee.org είναι authoritative για το συγκεκριμένο domain; Είναι ο name server που μας έχει απαντήσει authoritative για το συγκεκριμένο domain;

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματαΥπάρχει σημαία flag που προσδιορίζει αν ο name server είναι authoritative στο συγκεκριμένο domain και μάλιστα στο παράδειγμά μας o server που μας έχει απαντήσει δεν είναι (server is not an authoritative for domain).

1. Το όνομα www.ieee.org είναι domain name ή πρόκειται για canonical name;

Ένα όνομα τομέα είναι η διεύθυνση όπου οι internet users μπορούν να έχουν πρόσβαση στον ιστότοπό μας. Ένα domain name χρησιμοποιείται για την εύρεση και αναγνώριση υπολογιστών στο Διαδίκτυο. Οι υπολογιστές χρησιμοποιούν διευθύνσεις IP, οι οποίες είναι μια σειρά αριθμών. Ωστόσο, είναι δύσκολο για τους ανθρώπους να θυμούνται τις σειρές αριθμών. Εξαιτίας αυτού, τα ονόματα τομέα αναπτύχθηκαν και χρησιμοποιήθηκαν για τον εντοπισμό οντοτήτων στο Διαδίκτυο αντί για τη χρήση διευθύνσεων IP.

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματαΈνα canonical name είναι το σωστά δηλωμένο όνομα κεντρικού υπολογιστή ενός διακομιστή υπολογιστή ή δικτύου. Ένα CNAME καθορίζει ένα ψευδώνυμο για μια κανονική εγγραφή ονόματος κεντρικού υπολογιστή σε μια βάση δεδομένων του συστήματος ονομάτων τομέα (DNS). Κατά τον προγραμματισμό, ο όρος "canonical" σημαίνει "σύμφωνα με τους κανόνες". Το DNS είναι η τυπική μέθοδος καθορισμού των τοποθεσιών των τοποθεσιών στο Διαδίκτυο, ιδιαίτερα στις τοποθεσίες Web. Άρα το όνομα [www.ieee.org](http://www.ieee.org) είναι canonical name.

1. Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.ieee.org; Ποια είναι η IP διεύθυνση του δικού σας υπολογιστή;

Εικόνα που περιέχει στιγμιότυπο οθόνης

Περιγραφή που δημιουργήθηκε αυτόματαΗ IP διεύθυνση που αντιστοιχεί στον [www.ieee.org](http://www.ieee.org) είναι η 23.98.6.198

Η IP διεύθυνση που αντιστοιχεί στον δικό μου υπολογιστή είναι η 192.168.2.3

Εικόνα που περιέχει στιγμιότυπο οθόνης, κείμενο

Περιγραφή που δημιουργήθηκε αυτόματα

Ερωτήσεις σχετικά με το ICMP:

1. Πως θα δείτε μόνο τα πακέτα που αφορούν την επικοινωνία με βάση το πρωτόκολλο ICMP;
2. Εξετάστε το IP πακέτο που μεταφέρει το πρώτο ICMP Echo Request.
3. Ποια είναι η IP διεύθυνση του destination;
4. 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);
5. 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; 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;

Β’ ΜΕΡΟΣ

1. Ποια είναι η IP διεύθυνση που αντιστοιχεί στον www.ekt.gr;
2. Τα τρία πρώτα TCP segments που ανταλλάσσονται μεταξύ του υπολογιστή σας και του συστήματος που φιλοξενεί το www.ekt.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.
3. Εξετάστε τις θύρες (ports) προέλευσης (source) και προορισμού (destination) που χρησιμοποιήθηκαν από το HTTP πρωτόκολλο.
4. Πόσα πακέτα που περιείχαν HTTP GET αίτημα έστειλε ο browser σας; Προς ποιες IP διευθύνσεις στάλθηκαν τα μηνύματα αυτά;
5. Ποια έκδοση του HTTP τρέχει ο browser σας; Ποια έκδοση τρέχει ο server;