Δίκτυα Υπολογιστών: Εργαστηριακή Άσκηση 2

WIRESHARK

Σε αυτή την άσκηση θα ασχοληθούμε με εργαλεία ανάλυσης πακέτων. Συγκεκριμένα, αντικείμενο επεξεργασίας θα είναι το **wireshark,** το πιο διαδεδομένο εργαλείο ανάλυσης πακέτων (packet sniffer). Το **wireshark** είναι ένα πρόγραμμα που μπορεί να δει και να αναλύσει όλα τα πακέτα τα οποία στέλνονται μέσα σε ένα τοπικό δίκτυο. Μπορεί επομένως να χρησιμοποιηθεί τόσο για νόμιμες λειτουργίες διαχείρισης δικτύων όσο και για την κλοπή πληροφοριών από ένα δίκτυο. Τέτοιου είδους προγράμματα (ή συσκευές) είναι γνωστά ως sniffers και μπορούν να γίνουν εξαιρετικά επικίνδυνα για την ασφάλεια ενός δικτύου επειδή είναι ουσιαστικά αδύνατο να ανιχνευθούν και μπορούν να παρεμβληθούν σχεδόν οπουδήποτε.

Οι λειτουργίες του **wireshark** είναι οι εξής:

- Σύλληψη πακέτων δικτύου για λεπτομερειακή ανάλυση.
- Επόπτευση δικτυακής δραστηριότητας σε πραγματικό χρόνο.
- Συλλογή πληθώρας στατιστικών στοιχείων και παραμέτρων για επιμέρους σταθμούς, για συνομιλία σταθμών ακόμα και για μέρος του δικτύου.

Για περισσότερη βοήθεια μπορείτε να επισκεφτείτε και την ιστοσελίδα http://www.wireshark.org/ για πληροφορίες για το εργαλείο ανάλυσης πακέτων **wireshark**. Στόχος της άσκησης είναι η εξοικείωση με το **wireshark**. Οι βασικές λειτουργίες του **wireshark** στις οποίες θα εστιάσουμε την προσοχή μας είναι:

- **Παρατήρηση – Παρακολούθηση** (Monitoring) στατιστικών και λειτουργιών του δικτύου σε πραγματικό χρόνο.
- **Σύλληψη** (Capture) και **ανάλυση** πακέτων.

Μία σημαντική λειτουργία είναι η απεικόνιση στατιστικών στοιχείων με γραφικές παραστάσεις. Στις ακόλουθες υποενότητες θα περιγραφεί η διαδικασία για δύο ενδεικτικές παραμέτρους.

Δραστηριότητα 1: Χωρίς φίλτρο σύλληψης

1.1 Στη μπάρα του μενού που βρίσκεται στο πάνω μέρος της οθόνης πηγαίνουμε στην επιλογή **Capture►Options** και στη συνέχεια επιλέγουμε το κατάλληλο interface (οδηγό δικτύου) που χρησιμοποιεί ο υπολογιστής του εργαστηρίου και πατάμε OK. Μετέπειτα, διαμέσου της μπάρας μενού πηγαίνουμε στην επιλογή **Capture►Start**. Στο παράθυρο που εμφανίζεται πατάμε **OK** ώστε να αρχίσει η λειτουργία σύλληψης πακέτων. Μετά από 1 λεπτό απενεργοποιήστε τη λειτουργία σύλληψης. Μεταβείτε στην επιλογή **Statistics►IO Graphs** και: (α) Καταγράψτε την μέγιστη τιμή του γραφήματος για packets/tick (β) Καταγράψτε την μέγιστη τιμή του γραφήματος για bytes/tick

Δραστηριότητα 2: Φίλτρα σύλληψης & Παρατήρησης

2.1 Χρησιμοποιώντας ***φίλτρα σύλληψης***. Βρείτε και καταγράψτε την IP Address του υπολογιστή σας. Στη συνέχεια: επαναλάβετε την διαδικασία που περιγράφετε στην Δραστηριότητα 1 χρησιμοποιώντας αυτή τη φορά το φίλτρο σύλληψης: **host** (η IP Address του υπολογιστή σας). Τι παρατηρείτε;

2.2 Πέρα από τα φίλτρα σύλληψης μπορούν να χρησιμοποιηθούν και τα ***φίλτρα παρατήρησης***: Ενεργοποιήστε ξανά τη λειτουργία σύλληψης για 1 λεπτό. Πληκτρολογήστε την εντολή **ip.addr** == (η IP Address του υπολογιστή σας) στο πάνω αριστερό μέρος της οθόνης προγράμματος, στην περιοχή filter. Τι παρατηρείτε;

2.3 Ποια είναι η βασική διαφορά μεταξύ των φίλτρων παρατήρησης και των φίλτρων σύλληψης;

2.4 Μέσα από το μενού βοήθειας βρείτε δύο φίλτρα σύλληψης καθώς και δύο φίλτρα παρατήρησης (διαφορετικά από αυτά που χρησιμοποιήθηκαν παραπάνω) και εξηγείστε τη λειτουργία τους.

Δραστηριότητα 3: Αποκωδικοποίηση πακέτων

3.1 Είναι προφανές ότι η οθόνη χωρισμένη σε τρία μέρη. Τι δείχνει το κάθε μέρος;

Διαδικασία σύνδεσης υπολογιστή στο διαδίκτυο

Κάθε υπολογιστής συνδεμένος στο διαδίκτυο χαρακτηρίζεται από τρία στοιχεία:

- Το DNS όνομα του.

- Την IP διεύθυνση του.
- Την φυσική του διεύθυνση (MAC).

Η διαδικασία που ακολουθείται για να επικοινωνήσουμε με έναν υπολογιστή για τον οποίο γνωρίζουμε το DNS όνομα του (όπως για παράδειγμα για την επίσκεψη σε μια ιστοσελίδα η οποία είναι αποθηκευμένη σε ένα web server) είναι η εξής:

1. Καταρχήν ο υπολογιστής μας κάνει μια αίτηση στο τοπικό DNS εξυπηρετητή (server) για την αντιστοίχηση του ονόματος σε διεύθυνση IP.
2. Ο DNS εξυπηρετητής (server) απαντά με ένα μήνυμα το οποίο αντιστοιχίζει το όνομα που του δώσαμε με μία IP διεύθυνση.
3. Τελικά, το λογισμικό του χρήστη μαθαίνει τη IP διεύθυνση.
4. Αν ο υπολογιστής που θέλουμε να επικοινωνήσουμε βρίσκεται στο τοπικό υποδίκτυο τότε χρειαζόμαστε επιπλέον την φυσική του διεύθυνση. Για να γίνει αυτό στέλνετε ένα πακέτο σε όλους τους υπολογιστές του τοπικού δικτύου που ρωτά: "Σε ποιον ανήκει η IP διεύθυνση x.x.x.x ;". Το πακέτο θα φτάσει σε κάθε μηχανή του υποδικτύου και κάθε μία απ' αυτές θα ελέγξει για τη δική της διεύθυνση IP. Μόνο η μηχανή με τη σωστή διεύθυνση IP θα ανταποκριθεί δίνοντας την MAC διεύθυνσή της. ***Το πρωτόκολλο που διατυπώνει αυτή την ερώτηση και λαμβάνει την απάντηση είναι το ARP (Address Resolution Protocol)***.
5. Αν ο υπολογιστής που θέλουμε να επικοινωνήσουμε δεν βρίσκεται στο τοπικό υποδίκτυο τότε τα πακέτα στέλνονται συνήθως προς την Προεπιλεγμένη πύλη (**Default Gateway**) εξόδου από το τοπικό υποδίκτυο και δρομολογούνται προς την δοσμένη IP διεύθυνση.

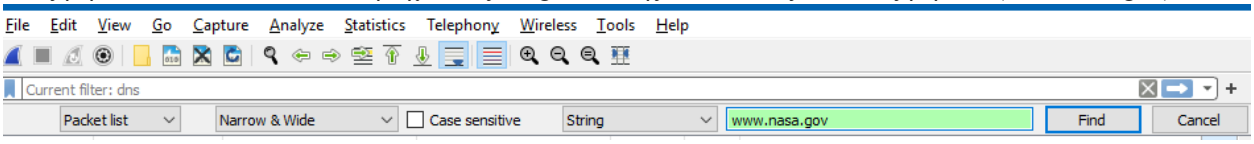
Ο υπολογιστής μας κράτα σε ένα (ARP) πίνακα κάθε μια από τις IP διευθύνσεις (και τις αντιστοιχίσεις τους σε φυσικές διευθύνσεις) για τις οποίες γίνεται επίλυση με τη βοήθεια του πρωτοκόλλου ARP.
Στην άσκηση αυτή θα παρατηρήσουμε την λειτουργία της εντολής ping με τη βοήθεια του **Wireshark**. Η εντολή **ping** ελέγχει εάν κάποιος κόμβος είναι ενεργός (*alive* ή *up*). ***Το ping χρησιμοποιεί το πρωτόκολλο ICMP (Internet Control Message Protocol)*** για να στείλει ένα πακέτο ECHO_REQUEST, έτσι ώστε να λάβει ένα ECHO_RESPONSE από τον συγκεκριμένο κόμβο. Κάθε φορά όμως που γίνεται ένα ping ενδέχεται να χρησιμοποιηθούν και κάποια άλλα από τα προαναφερθέντα πρωτόκολλα (διαδικασίες), εκτός του ICMP. Παρατηρήστε αυτές τις διαδικασίες εκτελώντας τα παρακάτω:

Δραστηριότητα 4: Wireshark - Εντολή ping

4.1 Εξηγείστε την λειτουργία των εντολών ping. ✓
4.2 Ενεργοποιείστε την σύλληψη πακέτων στο **Wireshark**. Ανοίξτε ένα παράθυρο γραμμής εντολής και ετοιμάστε μια απλή εντολή ping προς έναν από τους υπολογιστές του εργαστηρίου. Εκτελέσετε την εντολή. ✓
Καταγράψτε τα πρωτόκολλα που χρησιμοποιήθηκαν και τα είδη των μηνυμάτων που ανταλλάσσονται χρησιμοποιώντας την εντολή ping. (*Για να διευκολυνθείτε χρησιμοποιείστε ένα φίλτρο παρατήρησης **icmp**)
4.3 Βρείτε το πρώτο πακέτο echo_request από τον υπολογιστή σας προς τον υπολογιστή στόχο. Εντοπίστε και το πακέτο echo_reply που του αντιστοιχεί. Εξηγείστε τη στοίβα χρήσης των πρωτοκόλλων, σύμφωνα με την TCP/IP αρχιτεκτονική. ✓
4.4 Αναφέρετε τις βασικές πληροφορίες που περιείχε κάθε πακέτο που ανταλλάχθηκε. Για το πρωτόκολλο IP καταγράψτε τα στοιχεία του (Version, IHL - IP Header Length, Type of Service, Explicit Congestion Notification, Size of Datagram, Identification, Flags, Fragmentation Offset, Time To Live, Protocol, Header Checksum, Source Address, Destination Address, Options-εάν χρησιμοποιείται). Η απάντηση θα συνοδεύεται από screen-shot του wireshark όπου θα φαίνοται οι ανωτέρω πληροφορίες, αλλά και από κείμενο όπου θα δίνονται οι τιμές στις ανωτέρω παραμέτρους, π.χ. 0100 .... = Version: 4. Θα παρουσιάζεται και η αντιστοιχία της πληροφορίας σε bit στο πακέτο ✓
4.5 Επαναλάβετε το 4.4 κάνοντας ping με μέγεθος πακέτου 128. Αν δεν θυμάστε τον τρόπο να ρυθμίσετε το μέγεθος του echo_request, πληκτρολογήστε ping /? στη γραμμή εντολών ώστε να ανατρέξετε στη βοήθεια. ✓
a. Καταγράψτε τα στοιχεία της ερώτησης 4.4, ελέγξτε επίσης:
b. Ποια είναι η διαφορά ανάμεσα στο μέγεθος data που βλέπει το ICMP στην ερώτηση 4.3 και στο μέγεθος data που δείχνει τώρα;
c. Τι περιέχουν αυτά τα δεδομένα;

Δραστηριότητα 5: Wireshark – Επικοινωνία με εξυπηρετητή Ιστού

Ενεργοποιείστε την σύλληψη πακέτων στο **Wireshark** και στη συνέχεια ανοίξτε μια ιστοσελίδα την οποία δεν έχετε επισκεφτεί στο πρόσφατο παρελθόν, π.χ. www.nasa.gov (ή κάποια άλλη ιστοσελίδα της επιλογής σας). Περιμένετε λίγα λεπτά (2΄-3΄) και μετά κλείστε τον φυλλομετρητή. Μετά από άλλα 2΄ σταματήστε την σύλληψη πακέτων. Θέστε ως display filter το πρωτόκολλο dns και μετά μεταβείτε στο μενού Edit>Find Packet και αναζητήστε τα πακέτα τα οποία περιέχουν ως sting το url της ιστοσελίδας που αναζητήσατε (www.nasa.gov)



5.1 Επιλέξτε το πρώτο πακέτο και καταγράψτε τα πρωτόκολλα που χρησιμοποιούνται.
5.2 Συγκρίνετέ τα με τη μορφή της DNS επικεφαλίδας.
Βρείτε τα εξής στοιχεία για κάθε πακέτο: (α) ποιος είναι ο αποστολέας, (β) ποιος είναι ο παραλήπτης, (γ) ποιο είναι το μέγεθος του πακέτου, (δ) ποια πρωτόκολλα εμπλέκονται στην επικοινωνία, (ε) ποιες θύρες εμπλέκονται στην επικοινωνία, (στ) πώς υποβάλλεται το ερώτημα, (ζ) πώς επιστρέφεται η απάντηση;
5.3 Τα πρωτόκολλα που καταγράψατε σε ποιο επίπεδο ανήκουν σύμφωνα με το πρότυπο OSI;
5.4 Αλλάξτε το display filter σε http. Επιλέξτε στο **Wireshark** ένα πακέτο HTTP. Για αυτό το πακέτο καταγράψτε: το μέγεθος του, την IP διεύθυνση του αποστολέα, την IP διεύθυνση του παραλήπτη, ποιες θύρες (ports) χρησιμοποιήθηκαν από τον αποστολέα και τον παραλήπτη.
5.4 Εντοπίστε το πρώτο μήνυμα HTTP GET που έστειλε ο υπολογιστής σας για να κατεβάσει τη σελίδα και την αντίστοιχη απόκριση HTTP του εξυπηρετητή.
5.5 Στο πρώτο πλαίσιο που περιέχει πακέτο TCP, πιέστε το δεξί πλήκτρο του ποντικιού και επιλέξτε «Follow http Stream». Θα εμφανισθεί το περιεχόμενο της συγκεκριμένης ροής http, δηλαδή, της ανταλλαγή μηνυμάτων HTTP μεταξύ του πλοηγού και του εξυπηρετητή ιστού. Τα μηνύματα (εντολές) του πλοηγού ιστού εμφανίζονται σε ροζ φόντο, ενώ τα μηνύματα (αποκρίσεις) του εξυπηρετητή ιστού εμφανίζονται σε γαλάζιο φόντο.
5.6 Με εφαρμογή κατάλληλου φίλτρου εμφανίστε μόνο τα μηνύματα HTTP (http ή tcp.port == 80).
5.7 Θέλετε τώρα να δείτε μόνο τα μηνύματα HTTP που έστειλε ο υπολογιστής σας. Ποια είναι η σύνταξή του; [*Σημείωση: Για την ταυτόχρονη χρήση περισσότερων από ένα φίλτρο θα πρέπει να σχηματίσετε μια έκφραση με τον λογικό τελεστή ΚΑΙ (&&)*].

Δραστηριότητα 6: Wireshark – tracert vs pathping

6.1 Εξηγείστε την λειτουργία των εντολών tracert και pathping.
6.2 Ενεργοποιείστε την σύλληψη πακέτων στο **Wireshark** και στη συνέχεια εκτελέστε την εντολή tracert για έναν ιστότοπο της επιλογής σας. Καταγράψτε τα πρωτόκολλα που χρησιμοποιούνται κατά την επικοινωνία με την ιστοσελίδα και εξηγείστε συνοπτικά την χρήση τους.
6.3 Ενεργοποιείστε την σύλληψη πακέτων στο **Wireshark** και στη συνέχεια εκτελέστε την εντολή pathping για τον ιστότοπο που επιλέξατε και στην 3.1. Καταγράψτε τα πρωτόκολλα που χρησιμοποιούνται κατά την επικοινωνία με την ιστοσελίδα και εξηγείστε συνοπτικά την λειτουργία τους στο συγκεκριμένο παράδειγμα χρήσης.
6.4 Τι διαφορές παρατηρείτε μεταξύ tracert και pathping βάση της καταγραφής που κάνετε με την χρήση του Wireshark;

Δραστηριότητα 7: DHCP

7.1 Ενεργοποιείστε την σύλληψη πακέτων στο Wireshark και στη συνέχεια εκτελέστε την εντολή ipconfig /release και στην συνέχεια ipconfing /renew. Καταγράψτε τα πρωτόκολλα που χρησιμοποιούνται και εξηγείστε συνοπτικά την λειτουργία τους στο συγκεκριμένο παράδειγμα χρήσης.

Δραστηριότητα 8: Find my password

8.1 Βρείτε και συνδεθείτε σε κάποια δημόσια ανοικτή υπηρεσία όπως, για παράδειγμα, έναν ανοικτό εξυπηρετητή FTP που να επιτρέπει ανώνυμη πρόσβαση. Μια τέτοια περίπτωση είναι π.χ. το ftp.slackware.com. Ξεκινήστε την καταγραφή των πακέτων με το Wireshark και επισκεφτείτε την τοποθεσία στον φυλλομετρητή σας, δηλαδή το ftp://ftp.slackware.com/ . Όταν ολοκληρωθεί η διαδικασία σύνδεσης στον ftp server, σταματήστε την καταγραφή των πακέτων στο Wireshark. Για τον εντοπισμό του password στα πακέτα, χρησιμοποιήστε το φίλτρο tcp contains password ή το ftp κι επιλέξτε Apply. Έχοντας επιλέξει ένα από τα πακέτα που ξεχώρισε το φίλτρο, πηγαίνετε στο μενού Analyze κι επιλέξτε τη δυνατότητα Follow TCP stream. Με ποιο password συνδεθήκατε;

Foking done m8!!

Δίκτυα Υπολογιστών: Παραδοτέο της Εργαστηριακής Άσκησης 2

Παραδώστε σε κειμενογράφο επιλογής σας όλες τις απαντήσεις από τις παραπάνω δραστηριότητες (1-8) τηρώντας την αρίθμηση και την ταξινόμηση της άσκησης. Στην εργασία σας θα πρέπει να υπάρχουν τα αντίστοιχα screen shots από κάθε δραστηριότητα, καθώς και η πλήρη τεκμηρίωση τους.

Αναρτήστε τις απαντήσεις σας στον παρακάτω σύνδεσμο. Να είστε προσεκτικοί μόνον μια απάντηση ανά άτομο. Συμπιέστε το αρχείο πριν το αναρτήσετε.

https://docs.google.com/forms/d/e/1FAIpQLSfv6cwIFBEkMVhWwLrVCbStyyUfmoO6FTk9w0nLK15kYpjCmA/viewform?usp=pp_url

Ο σύνδεσμος θα είναι διαθέσιμος έως 01/05/2022 23.59.