ΗΜΥ 360
Εργαστηριακή Άσκηση 1
Βασικές Δυνατότητες Δικτύωσης
Wireshark: Αναλυτής Πρωτοκόλλων

Σκοπός της πρώτης σειράς ασκήσεων είναι, κατ' αρχήν, η εξοικείωση με τις βασικές δικτυακές δυνατότητες της οικογένειας λειτουργικών συστημάτων Linux και Microsoft Windows (παρόμοια εργαλεία υπάρχουν και στα δύο λειτουργικά). Επιπλέον, θα έχετε μια πρώτη επαφή με το wireshark, το οποίο είναι ένα εργαλείο ανάλυσης πρωτοκόλλων σε γραφικό περιβάλλον. Για την ανεύρεση των στοιχείων που ζητούνται στη συνέχεια, μπορείτε να χρησιμοποιήσετε είτε εντολές του λειτουργικού συστήματος ή πληροφορίες μέσω του γραφικού περιβάλλοντος.

Χρήσιμες εντολές φλοιού είναι οι `hostname`, `ifconfig`(Linux) ή `ipconfig` (Windows), net, netstat, nbtstat και route.

Το πρόγραμμα Wireshark είναι ένας ανιχνευτής πακέτων (packet sniffer) που διατίθεται ως ανοικτό λογισμικό (www.wireshark.com) για πληθώρα λειτουργικών συστημάτων. Η βασική του λειτουργία έγκειται στην σύλληψη των μηνυμάτων που στέλνονται ή λαμβάνονται από τον υπολογιστή σας. Τα περιεχόμενα των διαφόρων πεδίων των μηνυμάτων εμφανίζονται στην οθόνη αποκωδικοποιημένα. Μπορείτε για εξάσκηση να το εγκαταστήσετε και στον προσωπικό σας υπολογιστή κατεβάζοντας, ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείτε, το αντίστοιχο αρχείο από την ιστοσελίδα http://www.wireshark.com/download.html. Για να λειτουργήσει το Wireshark απαιτείται η ύπαρξη της βιβλιοθήκης σύλληψης πακέτων `libpcap`. Για συστήματα Windows η βιβλιοθήκη ονομάζεται WinPcap και εγκαθίσταται μαζί με το πρόγραμμα. Εναλλακτικά, μπορείτε να την κατεβάσετε από την ιστοσελίδα http://www.winpcap.org/. Περισσότερες πληροφορίες σχετικά με τον αναλυτή πρωτοκόλλων Wireshark μπορείτε να βρείτε στη σελίδα http://www.wireshark.com/docs/ όπου υπάρχουν σύνδεσμοι για το εγχειρίδιο χρήσης σε διάφορες μορφές (html, pdf, κλπ) καθώς και στην http://www.wireshark.com/faq.html σε περίπτωση που συναντήσετε δυσκολίες.

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα παραδοθεί στον επιβλέποντα.

Άσκηση 1: Βασικά χαρακτηριστικά των καρτών δικτύωσης.

Κάθε κάρτα δικτύου διαθέτει μια φυσική διεύθυνση, αυτήν του υποστρώματος MAC. Έχει μήκος 48 bit και η δομή της ορίζεται στο πρότυπο IEEE 802. Το πρώτο bit ορίζει το εάν πρόκειται για Ομαδική ή Ατομική διεύθυνση, το δεύτερο bit το εάν είναι Τοπική ή Μοναδική διεύθυνση, τα επόμενα 22 bit προσδιορίζουν τον κατασκευαστή της κάρτας και τα τελευταία 24 bit είναι ο αύξων αριθμός της κάρτας. Διεύθυνση με μόνο "11…1" υποδηλώνει εκπομπή (broadcast). Για τον υπολογιστή σας, βρείτε και καταγράψτε:

1. Την ονομασία της κάρτας δικτύωσης (network adapter)
2. Την ταχύτητα σύνδεσης.

3. Τη διεύθυνση υποστρώματος MAC σε δεκαεξαδική μορφή.
4. Τον κατασκευαστή της κάρτας δικτύωσης.
5. Τα συνδεδεμένα με αυτήν πρωτόκολλα δικτύωσης.
6. Τη διακοπή (interrupt – IRQ) που χρησιμοποιεί.

Άσκηση 2: Πρωτόκολλο επικοινωνίας TCP/IP.

Κάθε δικτυακή διεπαφή ενός host διαθέτει τη δική της διεύθυνση IP, η οποία είναι λογική (όχι φυσική). Οι δρομολογητές έχουν πολλαπλές διεπαφές και κάθε μία διαθέτει τη δική της διεύθυνση IP. Η τρέχουσα έκδοση του IP είναι η 4 και οι αντίστοιχες διευθύνσεις λέγονται IPv4. Αυτές έχουν μήκος 4 byte και δομή ιεραρχίας δύο επιπέδων:

1. Αριθμός δικτύου
2. Αριθμός host

Το όριο μεταξύ των επιπέδων αυτών, καθορίζεται από τη μάσκα υποδικτύου (subnet mask). Οι διευθύνσεις IP διακρίνονται από τα αρχικά bit της διεύθυνσης σε κατηγορίες (classes):

- 0: class A (πρώτο byte < 128)
- 10: class B (πρώτο byte στην περιοχή 128-191)
- 110: class C (πρώτο byte στην περιοχή 192-223)
- 1110: class D (πρώτο byte στην περιοχή 224-239)
- 11110: class E (πρώτο byte στην περιοχή 240-247)

Αφού μελετήσετε το help για τις εντολές `hostname`, `ifconfig` (Linux), `ipconfig` (Windows), `route`, `netstat`, `nbtstat` και `net`, δίνοντας έμφαση στις επιλογές `view` και `config` της τελευταίας, να απαντήσετε στα ακόλουθα ερωτήματα και να καταγράψετε μαζί με την απάντηση την ακριβή σύνταξη της εντολής που χρησιμοποιήθηκε:

1. Το όνομα του υπολογιστή σας.
2. Την περιοχή (Workstation/Logon domain) που ανήκει ο υπολογιστής σας.
3. Τη διεύθυνση IP του υπολογιστή σας
4. Την κατηγορία (class) που ανήκει η διεύθυνση IP του υπολογιστή σας.
5. Τη διεύθυνση υποστρώματος MAC.
6. Τη μάσκα του υποδικτύου.
7. Τη διεύθυνση IP της προκαθορισμένης πύλης (default gateway).
8. Το όνομα της περιοχής DNS.
9. Τη διεύθυνση IP του εξυπηρετητή DNS.
10. Τη διεύθυνση IP του εξυπηρετητή DHCP και τη διάρκεια της περιόδου απονομής (lease).
11. Τον αριθμό των πιο κάτω που στάλθηκαν/ελήφθησαν από τον υπολογιστή σας.
    1. πακέτων IP
    2. μηνυμάτων ICMP
    3. τμημάτων TCP
    4. δεδομενογραφημάτων UDP

help => `TCP/IP utilities.`

ipconfig /all
11 netstat –s netstat –n, netstat –o,

Άσκηση 3: **Αναλυτής Πρωτοκόλλων Wireshark.**

Η άσκηση αυτή αποτελεί εισαγωγή στη χρήση του αναλυτή πρωτοκόλλων Wireshark, του οποίου οι βασικές λειτουργίες είναι οι εξής: α) καταγραφή – σύλληψη (capture) και β) ανάλυση της δικτυακής κίνησης του υπολογιστή. Για κάθε λειτουργία ο χρήστης μπορεί να ορίσει κατάλληλα φίλτρα καταγραφής/ανάλυσης τα οποία περιορίζουν την κίνηση που καταγράφεται/αναλύεται σύμφωνα με τα κριτήριά του. Έτσι, σύμφωνα με την ορολογία του Wireshark διακρίνουμε τα capture και τα display filters αντίστοιχα, τα οποία θα αναλυθούν στις επόμενες σειρές ασκήσεων.

Ως εισαγωγικό παράδειγμα θα παρατηρήσετε την κίνηση που παράγεται από την επίσκεψη μιας ιστοσελίδας. Αφού ξεκινήσετε το Wireshark, οι διάφορες επιλογές που αφορούν τη λειτουργίας της καταγραφής ρυθμίζονται ακολουθώντας από το μενού επιλογών τη διαδρομή Capture | Options…). Στο παράθυρο που εμφανίζεται βεβαιωθείτε ότι στο πεδίο Interface αναφέρεται το όνομα της κάρτας δικτύου του υπολογιστή σας (ερώτημα 2.1) και επιπλέον ότι η επιλογή Enable network name resolution είναι ενεργοποιημένη. Πατώντας το Start αρχίζει η καταγραφή και εμφανίζεται σχετικό ενημερωτικό παράθυρο. Χρησιμοποιήστε ένα πλοηγό διαδικτύου (π.χ., firefox) για να επισκεφτείτε κάποια ιστοσελίδα, π.χ., http://ektor.telecom.ece.ntua.gr/. Μόλις φορτωθεί πλήρως η σελίδα πατήστε το Stop για να σταματήσει η καταγραφή. Στο κύριο παράθυρο του Wireshark, όπου φαίνεται η καταγεγραμμένη δικτυακή κίνηση, μπορεί ενδεχομένως να παρατηρήσετε κίνηση που δε σχετίζεται με την επίσκεψη της ιστοσελίδας. Η ζητούμενη κίνηση μπορεί να απομονωθεί με την εφαρμογή φίλτρου παρατήρησης ως εξής: πηγαίνετε Analyze | Display Filters… και πατήστε το πλήκτρο Expression. Από το πεδίο Field name βρείτε την επιλογή IP, πατήστε το +, διαλέγετε την επιλογή ip.addr, από το πεδίο Relation διαλέξτε το ==, στο πεδίο Value (IPv4 address) πληκτρολογήστε την διεύθυνση IP που σας ενδιαφέρει (π.χ., 194.42.10.196) και πατήστε OK. Το φίλτρο ενεργοποιείται με το πάτημα του Apply. Κλείνοντας το παράθυρο διαλόγου (με OK) θα διαπιστώσετε ότι η κίνηση είναι ενδεχομένως περιορισμένη σε σχέση με την παρατήρηση χωρίς φίλτρο.

1. Ποια είναι η διεύθυνση IP του ektor.telecom.ece.ntua.gr;
2. Να καταγράψετε τα πρωτόκολλα που παρατηρείτε ότι χρησιμοποιούνται για την επικοινωνία με την ιστοσελίδα.
3. Για καθένα από τα πρωτόκολλα του προηγούμενου ερωτήματος να γραφεί το επίπεδο που ανήκει σύμφωνα με το πρότυπο OSI.
4. Τοποθετήστε τον δρομέα στο πρώτο πακέτο TCP, πιέστε το δεξί πλήκτρο του ποντικιού και επιλέξτε το Follow TCP Stream. Στο παράθυρο που θα εμφανισθεί, παρουσιάζονται τα δεδομένα που μεταφέρθηκαν μέσω του TCP, στη συγκεκριμένη περίπτωση, τα μηνύματα πρωτοκόλλου http. Από το κείμενο που εμφανίζεται βρείτε:
    1. τον τύπο του εξυπηρετητή ιστού που φιλοξενεί τη σελίδα που επισκεφθήκατε,
    2. τον τίτλο και το αντίστοιχο HTML tag της σελίδας που επισκεφθήκατε
    3. Σε πιο σημείο του παραθύρου του browser εμφανίζεται αυτός ο τίτλος;
5. Ποια είναι η σύνταξη του φίλτρου που εμφανίζεται τώρα στο παράθυρο του φίλτρου ανάλυσης;