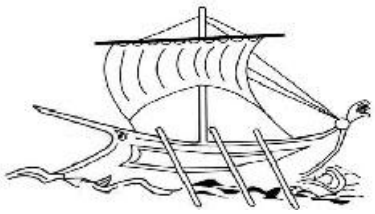


Ανώτατο Εκπαιδευτικό Ίδρυμα
Πειραιά Τεχνολογικού Τομέα
Τμήμα Ηλεκτρονικών Μηχανικών Τ.Ε.

Ανάλυση κίνησης σε τοπικό δίκτυο με χρήση αναλυτή πρωτοκόλλων

Πτυχιακή Εργασία

Φοιτητής: Παύλος Ψωμιάδης

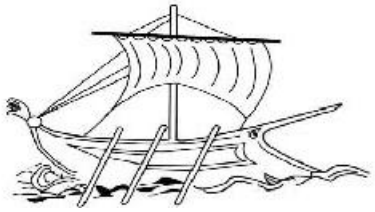
ΑΜ: 43406

Επιβλέπων Καθηγητής

Χαράλαμπος Πατρικάκης

Αναπληρωτής Καθηγητής στο Τομέα Επικοινωνιών και Δικτύων

Ημερομηνία:



Piraeus University
Of Applied Sciences
Department of Electronics Engineering

Traffic analysis over a Local Area Network (LAN) through the use of a protocol analyzer

Degree Thesis

Student: Paul Psomiadis

Registration Number: 43406

Supervisor

Charalampos Patrikakis

Associate Professor of Communications & Network Domain

Date:

Περίληψη

Η παρούσα πτυχιακή εργασία έχει ως αντικείμενο την ασφάλεια των δικτύων τόσο ενσύρματων όσο και ασύρματων. Ειδικότερα, θα ασχοληθεί με την παρακολούθηση και μελέτη διακίνησης πακέτων μέσα σε ένα δίκτυο ώστε να αναλυθεί η συμπεριφορά των χρηστών μέσα σε αυτό είτε είναι ομαλή είτε όχι. Η παρακολούθηση αυτή είναι εφικτή μέσω διαφόρων λογισμικών που ονομάζονται Packet Analyzers, τα οποία δρουν αιχμαλωτίζοντας τα πακέτα που εξέρχονται ή εισέρχονται στο δίκτυο.

Επιπλέον, θα αναλυθεί πληθώρα εννοιών που σχετίζονται άμεσα με την ασφάλεια δικτύων όπως είναι οι τέσσερις βασικές αρχές ασφάλειας δικτύων, δηλαδή εκείνη της Εμπιστευτικότητας (Confidentiality), Ιδιωτικότητας (Privacy), Διαθεσιμότητας (Availability) και Ακεραιότητας (Integrity). Ακόμα, θα γίνει λόγος σχετικά με τα είδη επιθέσεων του διαδικτύου όπως είναι οι επιθέσεις άρνησης υπηρεσίας (Denial of service), ενώ στη συνέχεια θα παρουσιαστούν τεχνολογίες αντιμετώπισης ανάλογων απειλών, όπως για παράδειγμα είναι η κρυπτογραφία τόσο συμμετρικού όσο και ασύμμετρου- δημόσιου κλειδιού, τα τείχη προστασίας ευρέως διαδεδομένα ως Firewalls καθώς και η τεχνολογία VPN (Virtual Private Network).

Είναι γνωστό ότι στη σύγχρονη εποχή, η τεχνολογία εξελίσσεται με πολύ γοργούς ρυθμούς με στόχο τη διευκόλυνση τόσο των ανθρώπων ως μεμονωμένων μονάδων όσο και ως μελών μιας ομάδας όπως είναι ένας οργανισμός ή μια επιχείρηση. Αναφερόμενοι στην τεχνολογία θα ήταν παράλειψη αν δε γινόταν μνεία στα δίκτυα. Με τον ορό δίκτυα σε εννοούμε ουσιαστικά την επικοινωνία των μελών τόσο εσωτερικά με τους συνάδελφους όσο και με εξωτερικούς συνεργάτες μέσω διαδικτύου. Είναι κατανοητό λοιπόν ότι η επικοινωνία καθορίζει την ομαλή λειτουργία καθώς και την ανάπτυξη μιας επιχείρησης-οργανισμού. Επομένως, η ασφάλεια της επικοινωνίας αυτής, αυστηρά συνυφασμένη με την ασφάλεια του δικτύου, είναι αποφασιστικής σημασίας ώστε να μην εμπλακούν εξωτερικοί παράγοντες που έχουν σκοπό να βλάψουν την επιχείρηση ή οργανισμό.

Τέλος, η παρούσα πτυχιακή δε θα αρκεστεί αποκλειστικά σε θεωρητικό επίπεδο καθώς το κύριο θέμα με το οποίο θα ασχοληθεί όπως ειπώθηκε ανωτέρω αποτελεί τα packet analyzers, γνωστά και ως network analyzers, protocol analyzers, packet sniffers ή αλλιώς στα ελληνικά λογισμικά ανάλυσης πρωτοκόλλων δικτύων υπολογιστών. Εκείνα παρέχουν τη δυνατότητα παρακολούθησης των πακέτων ενός δικτύου και όταν γίνει αντιληπτό κάποιο πακέτο το οποίο ικανοποιεί συγκεκριμένα κριτήρια, καταγράφεται σε ένα αρχείο. Ανάμεσα στη πληθώρα λογισμικών, το πιο ευρέως διαδεδομένο και γνωστό όμως είναι το Wireshark το οποίο επίσης είναι και ελεύθερο. Χρησιμοποιώντας λοιπόν το Wireshark θα γίνει προσπάθεια να αναλύσουμε τα πακέτα που αιχμαλωτίζει το συγκεκριμένο λογισμικό, ώστε να γίνει κατανοητή η κίνηση που υπάρχει στο δίκτυο από το κάθε χρήστη.

Abstract

The purpose of this thesis is to deal with security issues regarding wireless and wired networks, more specifically it will deal with issues such as interception and log traffic that passes over a digital network or part of a network, in order to analyze the behavior of each user so as to check if it is normal or not. This can be achieved by using some computer programs known as Packet Analyzers which function is carried out by capturing the traffic and the packets that flow across the network.

Furthermore, several concepts that are directly related to network security, such as the four basic principles of network security, which are the Confidentiality, Privacy, Availability, and Integrity, will be analyzed. In addition, kinds of Internet attacks such as Denial of Service and then some technologies to deal with such threats, like cryptography of both symmetric and asymmetric-public keys, Firewalls, VPN (Virtual Private Network), and more will be presented.

It is well known that nowadays technology is progressing rapidly so it can make our lives better and easier. Networks are a big part of technology that is developing more and more throughout the years and they are becoming a huge and important part for both humans and companies or organizations. With the term of networks inside a company, we actually mean the communication that occurs either inside the company among the members of the company or outside of it, with some outside associates for instance. It is clear to see that the communication serves to smooth operation and development of the company. In order to achieve this purpose it is needed to have a safe communication which is the same as a safe network, so that any action with bad intentions is prevented.

Finally, the present diploma will not be exclusively restricted in theoretical issues , as the main issue is to deal with the packet analyzers, also known as network analyzers, protocol analyzers, packet sniffers.

They are capable of monitoring the packets of a network, and when a packet that meets specific criteria is perceived, it is recorded in a file. Among different types of software, the most widespread and well known is Wireshark which is also free. Therefore, using Wireshark, there will be an effort to analyze the packages captured by this particular software, which are of course encrypted, in order to understand the behavior of each user.