ΑΛΕΞΑΝΔΡΕΙΟ Τ. Ε. Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Network Forensics

Του φοιτητή: **ΓΙΑΛΟΥΡΗ ΚΩΝΣΤΑΝΤΙΝΟΥ**

Επιβλέπων καθηγητής: **ΗΛΙΟΥΔΗΣ ΧΡΗΣΤΟΣ**

ΘΕΣΣΑΛΟΝΙΚΗ, 2009

Στους γονείς μου Γιώργο και Λία

και στον αδερφό μου Παναγιώτη

Πρόλογος

Αντικείμενο της παρούσας πτυχιακής εργασίας, είναι η διερεύνηση των παραβιάσεων ασφαλείας δικτύων. Τα τελευταία χρόνια εμφανίστηκε μια νέα προσέγγιση-επέκταση της ασφάλειας δικτύων υπό τον όρο Network Forensics ή αλλιώς Δικανική Δικτύων. Κύριος λόγος της εμφάνισης του πεδίου Network Forensics, ήταν η ανάγκη υποστήριξης των μηχανισμών ασφαλείας με δυνατότητες περαιτέρω διερεύνησης, μετά την αναγνώριση μιας παραβίασης ή εισβολής στο δίκτυο. Αυτή η νέα προσέγγιση δίνει έμφαση στις δυνατότητες διερεύνησης των παραβιάσεων και των συμβάντων που απειλούν την ασφάλεια του δικτύου. Το πεδίο του Network Forensics, επικεντρώνεται στις τεχνικές σύλληψης, καταγραφής και ανάλυσης των δικτυακών πακέτων για την διεξαγωγή έρευνας και την εξαγωγή συμπερασμάτων.

Παρόλο που το πεδίο του Network Forensics, είναι αρκετά νέο και λίγη έρευνα έχει διεξαχθεί πάνω σε αυτό, έγινε προσπάθεια ώστε να μελετηθούν και να καταγραφούν οι μεθοδολογίες και τα μοντέλα Network Forensics, έτσι όπως προτάθηκαν από ερευνητές του χώρου. Ελλείψει προτυποποίησης, επιχειρείται μια εισαγωγή στις βασικές έννοιες, στα εργαλεία και στα μοντέλα που μπορούν να χρησιμοποιηθούν και να προσφέρουν καθοδήγηση στη διαδικασία του Network Forensics.

Τέλος, θα ήθελα να ευχαριστήσω ιδιαίτερα, τον επιβλέποντα καθηγητή μου κ. Ηλιούδη Χρήστο, για την καθοδήγησή του στην συγγραφή αυτής της πτυχιακής, τη βοήθειά του στην εύρεση βιβλιογραφικού υλικού, στην οργάνωση της πτυχιακής, τις διορθώσεις και γενικά για το χρόνο που διέθεσε, καθώς και για την ανάθεση του θέματος της πτυχιακής. Επίσης, θα ήθελα να ευχαριστήσω τον συμφοιτητή μου Θεοδώρου Κωνσταντίνο, για τις συμβουλές και τη βοήθεια του στην υλοποίηση της εφαρμογής.

Περίληψη

Το πεδίο της Δικανικής Δικτύων (Network Forensics) αποτελεί μια νέα προσέγγιση της ασφάλειας δικτύων. Κύριος λόγος της εμφάνισης του πεδίου Network Forensics, ήταν η ανάγκη υποστήριξης των μηχανισμών ασφαλείας με δυνατότητες περαιτέρω διερεύνησης, μετά την αναγνώριση μιας παραβίασης ή εισβολής στο δίκτυο.

Στο πρώτο κεφάλαιο, παρουσιάζεται το πεδίο της Δικανικής Υπολογιστών (Computer Forensics), ένας ευρύτερος κλάδος στον οποίο ανήκει η Δικανική Δικτύων. Η Δικανική Υπολογιστών ασχολείται με τη συλλογή ψηφιακών αποδεικτικών στοιχείων από Ηλεκτρονικούς Υπολογιστές και γενικότερα ψηφιακές αποθηκευτικές συσκευές. Η μεθοδολογία που ακολουθείται περιλαμβάνει τέσσερεις φάσεις που αποτελούν αυτή τη διαδικασία: τη φάση της συλλογής, της εξέτασης, της ανάλυσης και της αναφοράς των αποτελεσμάτων. Περιγράφονται οι κύριες πηγές δεδομένων σε ένα υπολογιστή, τεχνικές για την περισυλλογή των δεδομένων, κατηγοριοποίηση τους με βάση την ευαισθησία των εκάστοτε δεδομένων σε αλλοιώσεις και τροποποιήσεις.

Το δεύτερο κεφάλαιο ξεκινά με μια εισαγωγή στην Δικανική Δικτύων, δίνοντας κάποιους ορισμούς, παρουσιάζει τις κυριότερες πηγές δικτυακής κίνησης και γίνεται η διαφοροποίηση της Δικανική Δικτύων από τη Δικανική Υπολογιστών. Εν συνεχεία, περιγράφονται κάποια μοντέλα και αρχιτεκτονικές, τα οποία παρουσιάζουν διάφορες μεθοδολογίες για τους τρόπους συλλογής των στοιχείων από το δίκτυο, αποθήκευσης και ανάλυσης τους.

Το τρίτο κεφάλαιο ασχολείται με τα εργαλεία (εμπορικά και ανοιχτού κώδικα) και τις τεχνικές υποστήριξης της Δικανικής Δικτύων. Πιο συγκεκριμένα, περιγράφονται οι κυριότερες τεχνικές sniffing και το περιβάλλον στο οποίο μπορούν να εφαρμοστούν, οι πιο δημοφιλείς packet sniffers, packet analyzers και NFAT εργαλεία, με τις βασικές λειτουργίες που υποστηρίζουν και τις δυνατότητες που παρέχουν.

Τέλος, δε θα μπορούσε να παραληφθεί η ασύρματη εκδοχή της Δικανικής Δικτύων, η οποία παρουσιάζεται στο τέταρτο κεφάλαιο. Περιγράφονται τα

ζητήματα που σχετίζονται με αυτή, τις τεχνικές δυσκολίες και τις προκλήσεις που παρουσιάζει η συλλογή της δικτυακής κίνησης στα ασύρματα δίκτυα και προτείνονται κάποιες τεχνικές και για την καλύτερη σχεδίαση εργαλείων ασύρματης δικανικής. Τελειώνοντας, στο πέμπτο κεφάλαιο παρουσιάζονται τα κίνητρα και οι προκλήσεις που συναντώνται στην προσπάθεια ενσωμάτωσης της Δικανικής Δικτύων στις υποδομές των δικτύων. Λόγω της νεότητας του πεδίου, είναι απαραίτητη η επισήμανση κάποιων ζητημάτων που χρειάζονται περαιτέρω έρευνα και στα οποία υπάρχουν ελλείψεις, ενώ συνοψίζονται τα κύρια συμπεράσματα που εξάχθηκαν με την περάτωση αυτής της πτυχιακής.

Abstract

The goal of this project is to examine network intrusions, by following a new approach to the network security field, known under the term Network Forensics. Network Forensics is an important extension to the model of network security where emphasis is more commonly put on prevention and to a lesser extent on detection. It focuses on the capture, recording and analysis of network packets and events for investigative purposes.

The first chapter introduces the reader to the field of Computer Forensics that is the application of science to the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining the chain of custody for the data.

The second chapter starts with an introduction to the field of Network Forensics, giving some terms and definitions and differentiates Network Forensics from Computer Forensics. The second half of this chapter presents some proposed models of Network Forensics and the implementation architectures.

Chapter three focuses on the tools (open source and commercial) that could be used for the purpose of Network Forensics. More specifically, the tools required to collect and analyze network traffic, are described, demonstrating some of the basic supported capabilities.

The fourth chapter addresses the main considerations and challenges that are inserted from the adoption of wireless technology, forming the field of Wireless Forensics, the state of the art in Network Forensics.

Finally, the last chapter concludes the project by presenting the motives and the challenges to overcome, in order to integrate forensic capabilities into the networks infrastructures. Aside from that, some major issues are high-lighted for future research.

Ευρετήριο Περιεχομένων

Ευρετήριο Σχημάτων – Πινάκων

ΚΕΦΑΛΑΙΟ 1

Computer Forensics – Δικανική Υπολογιστών

Η ολοένα και περισσότερο αυξανόμενη χρήση των νέων τεχνολογιών, της πληροφορικής και του διαδικτύου σε συνδυασμό με την μεγάλη επεξεργαστική ισχύ των σύγχρονων υπολογιστών αλλά και την τεράστια αποθηκευτική ικανότητα των σκληρών δίσκων έχει οδηγήσει σε νέους τρόπους διάδοσης και εξάπλωσης της πληροφορίας. Καθημερινά προστίθενται νέοι υπολογιστές αλλά και δίκτυα στο διαδίκτυο (Internet) προκειμένου όλοι να επωφεληθούν από τις τεράστιες δυνατότητες επικοινωνίας και πληροφόρησης που αυτό προσφέρει. Τα ίδια όμως τεχνολογικά επιτεύγματα μπορούν να χρησιμοποιηθούν από κάποιους για κακόβουλους σκοπούς.

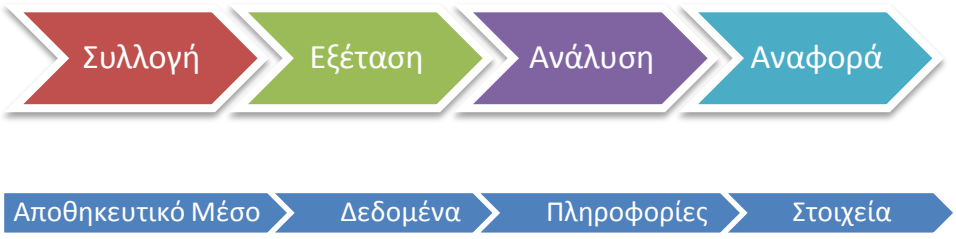
1.1 Εισαγωγή στη Δικανική Υπολογιστών

Ο όρος Δικανική Υπολογιστών (Computer Forensics ή αλλιώς Digital Forensics) αναφέρεται σε ένα κλάδο της Δικανικής Επιστήμης (Science Forensic, της επιστήμης δηλαδή που ασχολείται με την συλλογή αποδεικτικών στοιχείων σε εγκληματικές και παραβατικές ενέργειες) ο οποίος αποτελεί τη μεθοδολογία η οποία ακολουθείται για την συλλογή ψηφιακών αποδεικτικών στοιχείων από Ηλεκτρονικούς Υπολογιστές και γενικότερα ψηφιακές αποθηκευτικές συσκευές. Η ευρεία χρήση και ποικιλία των διάφορων ηλεκτρονικών συσκευών που χρησιμοποιούνται στην καθημερινή ζωή έχει ως αποτέλεσμα ένα μεγάλο αριθμό πηγών από όπου μπορούμε να συλλέξουμε δεδομένα [E11, E115]. Ως δεδομένο θεωρείται οτιδήποτε βρίσκεται σε κατάλληλη μορφή ώστε να μπορεί χρησιμοποιηθεί από έναν ηλεκτρονικό υπολογιστή ή κάποια άλλη ηλεκτρονική συσκευή. Τα δεδομένα δεν έχουν όλα την ίδια μορφή αλλά μπορούν να αποθηκευθούν μαζικά. Ηλεκτρονικοί Υπολογιστές, δικτυακές συσκευές, περιφερειακά υπολογιστών, PDA (personal digital assistants), CD, DVD, εξωτερικοί σκληροί δίσκοι , μνήμες flash, κινητά τηλέφωνα και ψηφιακές κάμερες

είναι μερικές μόνο από τις συσκευές όπου αποθηκεύονται δεδομένα. Ύστερα από επεξεργασία των δεδομένων μπορούμε να εξάγουμε την πληροφορία που μας ενδιαφέρει. Από τη φύση τους τα ψηφιακά δεδομένα είναι πολύ ευάλωτα και μπορούν εύκολα να αλλαχθούν, να διαγραφούν ή να καταστραφούν ακόμα και να αγνοηθούν αν δεν γίνει σωστός χειρισμός τους [NIJ08, SOL04, IJC08].

1.2 Η Δικανική Διαδικασία

Ως Διαδικασία της Δικανικής Υπολογιστών (Computer Forensic Process) θα μπορούσε να χαρακτηριστεί η διαδικασία που ακολουθείται, έτσι ώστε από το υπολογιστικό σύστημα που μας ενδιαφέρει να μπορέσουμε να εξάγουμε κάποια αποδεικτικά στοιχεία [NIS86]. Οποιοσδήποτε και αν είναι ο σκοπός της συλλογής των αποδεικτικών στοιχείων, ειδικά μέτρα πρέπει να λαμβάνονται κατά την διάρκεια της όλης διαδικασίας ώστε να διατηρείται η ακεραιότητα των δεδομένων και κυρίως στις περιπτώσεις όπου τα στοιχεία αυτά θα πρέπει να γίνουν αποδεκτά από το δικαστήριο. Η μεθοδολογία και ο σκοπός της Δικανικής Υπολογιστών δεν είναι ίδιος με την απλή ανάκτηση χαμένων δεδομένων (data recovery), αλλά να εξαχθούν όσο το δυνατόν περισσότερες πληροφορίες που να αφορούν αυτά τα δεδομένα. Στην περίπτωση παραβίασης ενός υπολογιστικού συστήματος από κάποιο επιτιθέμενο, σκοπός είναι να προσδιοριστεί ο τρόπος με τον οποίο κατάφερε να αποκτήσει πρόσβαση στο σύστημα, ποίες ήταν οι ενέργειες του πάνω σε αυτό και ποιός ήταν ο στόχος-αιτία της επίθεσης. Εν συντομία οι τέσσερεις φάσεις που αποτελούν αυτή τη διαδικασία είναι, η φάση της συλλογής (Collection), της εξέτασης (Examination), της ανάλυσης (Analysis) και της αναφοράς των αποτελεσμάτων (Reporting).



Εικόνα 1.1. Η διαδικασία της Δικανικής Υπολογιστών

1.2.1 Συλλογή των δεδομένων

Πριν ξεκινήσει οποιαδήποτε ενέργεια σε ένα υπό εξέταση σύστημα, πρέπει να ληφθούν κάποια μέτρα ώστε να μην υπάρξουν εξωτερικοί παράγοντες που θα τροποποιήσουν ή θα διαγράψουν σημαντικά στοιχεία του συστήματος. Συστήματα τα οποία βρίσκονται σε λειτουργία θα πρέπει να συνεχίσουν να είναι σε λειτουργία, μέχρις ότου συλλεχθούν όλα εκείνα τα ευμετάβλητα δεδομένα που υπάρχουν στη μνήμη του συστήματος και αφορούν δεδομένα του λειτουργικού συστήματος είτε των εφαρμογών που χρησιμοποιήθηκαν. Η μνήμη μπορεί να περιέχει πολύ χρήσιμα στοιχεία τα οποία μπορούν να χρησιμοποιηθούν στη συνέχεια όπως, ενεργές εφαρμογές, συνδέσεις και πόρτες, δικτύου κωδικοί πρόσβασης, κλειδιά κρυπτογράφησης δεδομένων, e-mail και άλλα στοιχεία που μαρτυρούν τις δραστηριότητες του χρήστη. Κάποιες φορές τέτοιου είδους στοιχεία μπορούν να βρεθούν σε σημειωματάρια ή σε αυτοκόλλητες σημειώσεις στον ίδιο χώρο που βρίσκεται και το σύστημα που μας ενδιαφέρει. Αφού τα ασταθή δεδομένα συλλεχθούν, η απενεργοποίηση του συστήματος δεν πρέπει να γίνει με τον παραδοσιακό τρόπο τερματισμού λειτουργίας αλλά αντιθέτως θα πρέπει να αφαιρεθεί ξαφνικά η τροφοδοσία ρεύματος έτσι ώστε να αποτρέψουμε εγγραφές δεδομένων στο σκληρό δίσκο. Σε αυτό το σημείο είναι χρήσιμο να αναφερθεί ότι τα δεδομένα ενός σκληρού δίσκου τα οποία θεωρούνται διαγραμμένα από το σύστημα στην πραγματικότητα δεν διαγράφονται αλλά μπορούν να διαβαστούν εφόσον δεν έχει γίνει επανεγγραφή άλλων δεδομένων πάνω σε αυτά [BRO07, IJC08].

1.2.1.1 Αναγνώριση των πιθανών πηγών δεδομένων

Το πρώτο βήμα σε αυτή την φάση είναι η αναγνώριση πιθανών πηγών δεδομένων και η εξαγωγή των δεδομένων αυτών. Η ευρεία αποδοχή των ψηφιακών συσκευών και της σύγχρονης τεχνολογίας, από μεγάλο σύνολο του απλού χρήστη, και η χρησιμοποίηση τους στην καθημερινή ζωή έχει οδηγήσει σε υπερπληθώρα πιθανών πηγών δεδομένων. Παρόλα αυτά οι πιο κοινές και συνηθέστερες πηγές δεδομένων είναι οι επιτραπέζιοι και φορητοί υπολογιστές καθώς και οι διάφορες

αποθηκευτικές συσκευές. Τα περισσότερα συστήματα μπορούν να δεχτούν οπτικούς δίσκους (CD,DVD) αλλά επίσης διαθέτουν διαφόρων ειδών θύρες όπως η USB (Universal Serial Bus), η Firewire, η PCMCIA (Personal Computer Memory Card International Association), η e-SATA (external Serial Advanced Technology Attachment) στις οποίες εξωτερικά αποθηκευτικά μέσα και άλλες συσκευές μπορούν να συνδεθούν. Φυσικά, τα υπολογιστικά συστήματα διαθέτουν και άλλες πηγές δεδομένων, τα δεδομένα των οποίων είναι ευμετάβλητα και προσωρινά διαθέσιμα ή διαθέσιμα υπό συγκεκριμένες συνθήκες. Ένα τέτοιο παράδειγμα είναι τα δεδομένα που βρίσκονται στην μνήμη RAM του υπολογιστή, η οποία φυλάσσει προσωρινά κάποια δεδομένα μέχρι κάποια άλλα να πάρουν τη θέση τους ή μέχρι να διακοπεί η παροχή ρεύματος. Τα στοιχεία που θα συλλεχθούν δεν προέρχονται απαραίτητα από πηγές δεδομένων που βρίσκονται σε συγκεκριμένο χώρο, καθώς οι δικτυωμένοι υπολογιστές έρχονται σε επικοινωνία με άλλους απομακρυσμένους υπολογιστές οι οποίοι μπορεί να περιέχουν σημαντικά στοιχεία.

Τα περισσότερα λειτουργικά συστήματα μπορούν να ρυθμιστούν έτσι ώστε να παρακολουθούν και να καταγράφουν συγκεκριμένες ενέργειες που συμβαίνουν στο σύστημα, οι οποίες καθορίζονται από το διαχειριστή του συστήματος. Για παράδειγμα οι προσπάθειες αυθεντικοποίησης ενός χρήστη, οι αλλαγές στην πολιτική ασφαλείας ή άλλα ύποπτα συμβάντα, μπορούν να καταγράφονται σε αρχεία καταγραφής (log files) και να παρέχουν χρήσιμες πληροφορίες όπως, η ώρα στην οποία πραγματοποιήθηκε ένα γεγονός και αυτό που το προκάλεσε. Σε μερικά συστήματα και στα περισσότερα δίκτυα υπολογιστών αντίγραφα αυτών των αρχείων προωθούνται και αποθηκεύονται σε κεντρικούς εξυπηρετητές (log servers) ώστε να εξασφαλίζεται η ακεραιότητα τους. Δημιουργώντας αντίγραφα ασφαλείας των αρχείων καταγραφής (log files) και εξετάζοντας τακτικά το περιεχόμενο τους αλλά και η παρατήρηση σε πραγματικό χρόνο, βοηθάει στη σκιαγράφηση του συστήματος. Παρατηρώντας τις δραστηριότητες ενός συστήματος και τη συμπεριφορά των χρηστών του, διευκολύνει τον εντοπισμό ασυνήθιστων ενεργειών και απόπειρες παραβίασης του συστήματος.

1.2.1.2 Απόκτηση των δεδομένων

Μετά τον εντοπισμό των πιθανών πηγών δεδομένων, σειρά έχει η εξόρυξη των δεδομένων. Επειδή τα δεδομένα που ενδιαφέρουν κάθε φορά και ο σκοπός εξόρυξης τους δεν είναι πάντοτε ο ίδιος, πρέπει πρώτα σχεδιαστεί ένα πλάνο τριών βημάτων το οποίο θα χρησιμοποιηθεί στη συνέχεια για την απόκτηση των δεδομένων.

1. Εξαιτίας των πολλών πηγών δεδομένων (και ίσως του περιορισμένου χρόνου που είναι διαθέσιμος) πρέπει να εκτιμηθεί η προτεραιότητα που θα έχει η κάθε πηγή για την εξόρυξη των δεδομένων. Το πρώτο πράγμα που θα πρέπει να εκτιμηθεί είναι η “αξία” που θα έχουν τα δεδομένα από μια συγκεκριμένη πηγή. Για παράδειγμα, η εξόρυξη δεδομένων από ένα σκληρό δίσκο είναι μια χρονοβόρα διαδικασία η οποία ίσως να μην δώσει σημαντικές πληροφορίες. Σε κάθε περίπτωση η εμπειρία του αναλυτή έχει τον πρώτο λόγο. Ένας δεύτερος παράγοντας είναι η μεταβλητότητα που παρουσιάζουν τα δεδομένα. Τα μεταβλητά δεδομένα (volatile data) αφορούν τα δεδομένα ενός συστήματος που βρίσκεται σε λειτουργία (live system) και τα οποία θα χαθούν αν το σύστημα τεθεί εκτός λειτουργίας. Μερικές φορές τα μεταβλητά δεδομένα μπορούν να χαθούν εξαιτίας ενεργειών που πραγματοποιήθηκαν στο σύστημα. Στις περισσότερες περιπτώσεις τα μεταβλητά δεδομένα έχουν μεγαλύτερη προτεραιότητα από τα μόνιμα αποθηκευμένα δεδομένα (non-volatile data), ωστόσο μερικές φορές τα μόνιμα αποθηκευμένα δεδομένα, είναι δυναμικά και μπορεί να αντικατασταθούν από άλλα όπως για παράδειγμα τα πιο πρόσφατα αρχεία καταγραφής (log files) να αντικαταστήσουν τα παλιότερα.

2. Για την εξόρυξη των δεδομένων χρησιμοποιούνται διάφορα εργαλεία ανάλυσης (analysis - forensic tools) τα οποία δημιουργούν ακριβή αντίγραφα των δεδομένων πάνω στα οποία θα γίνει η ανάλυση των δεδομένων. Η πρόσβαση στα δεδομένα ενός συστήματος μπορεί να

γίνει είτε τοπικά είτε μέσω δικτύου. Παρόλο που η συλλογή δεδομένων τοπικά μας δίνει μεγαλύτερο έλεγχο στο σύστημα και μπορούμε ευκολότερα να αποτρέψουμε εξωτερικές παρεμβάσεις προς το σύστημα (με στόχο την αλλοίωση των δεδομένων), αυτό δεν είναι πάντοτε εφικτό. Σε αυτές τις περιπτώσεις η συλλογή των δεδομένων από απομακρυσμένα συστήματα γίνεται μέσω δικτύου.

3. Μετά την ολοκλήρωση της συλλογής των δεδομένων από κάθε πιθανή πηγή και της δημιουργίας ακριβή αντιγράφων τους πάνω στα οποία θα πραγματοποιηθεί η ανάλυση των δεδομένων, είναι απαραίτητο να εξασφαλιστεί ότι τα αντίγραφα είναι όντως ακριβή και ότι περιέχουν ακριβώς τα ίδια δεδομένα, bit προς bit. Για να γίνει αυτό ειδικά εργαλεία χρησιμοποιούνται για να υπολογίσουν τη σύνοψη μηνύματος (message digest) των αρχικών δεδομένων και από τα αντίγραφα των δεδομένων αντίστοιχα. Σε περίπτωση που αυτά διαφέρουν, τότε υπήρξε κάποια αλλοίωση των δεδομένων.

1.2.2 Εξέταση των δεδομένων

Σε αυτή τη φάση τα δεδομένα που έχουν συγκεντρωθεί θα πρέπει να εξεταστούν ώστε να εξαχθούν από αυτά χρήσιμες πληροφορίες. Τις περισσότερες φορές διάφορες δυσκολίες θα πρέπει να ξεπεραστούν καθώς τα δεδομένα μπορεί να βρίσκονται σε συμπιεσμένη μορφή ή να είναι κρυπτογραφημένα και να απαιτείται κάποιο κλειδί ώστε να αποκρυπτογραφηθούν ή να προστατεύονται από κάποιο μηχανισμό ελέγχου πρόσβασης. Λόγω του μεγάλου αριθμού αρχείων που πιθανότατα συλλέχθηκαν θα πρέπει να βρεθούν αρχεία με πληροφορίες που παρουσιάζουν ενδιαφέρον. Επίσης σε ένα αρχείο, μπορεί πολλές από τις πληροφορίες που περιέχει να μην ενδιαφέρουν και να χρειαστεί φιλτράρισμα ώστε να απομείνουν μόνο κάποιες συγκεκριμένες πληροφορίες. Για παράδειγμα το αρχείο καταγραφής (log file) ενός τείχους προστασίας (firewall) μπορεί να φιλτραριστεί ώστε να εμφανίζει γεγονότα που συνέβησαν μια συγκεκριμένη χρονική περίοδο. Χρησιμοποιώντας κάποιες άλλες τεχνικές φιλτραρίσματος είναι δυνατόν να μειωθεί σημαντικά ο όγκος των προς εξέταση δεδομένων. Η

αναζήτηση με χρήση προτύπων με στόχο την εξαγωγή συγκεκριμένων αποτελεσμάτων είναι μια από αυτές τις τεχνικές. Μια επίσης χρήσιμη τεχνική είναι ο προσδιορισμός του τύπου των περιεχομένων κάθε αρχείου δεδομένων με χρήση εξειδικευμένων εργαλείων (η κατάληξη ενός αρχείου δεν αποτελεί εγγύηση για τον τύπο του αρχείου). Ένα αρχείο μουσικής μπορεί να μην παρουσιάζει ενδιαφέρον ενώ αντίθετα αρχεία κειμένου, γραφικών ή συμπιεσμένα αρχεία να απαιτούν περαιτέρω εξέταση.

1.2.3 Ανάλυση των δεδομένων

Αφού έχουν εξαχθεί πλέον οι πληροφορίες που παρουσιάζουν ενδιαφέρον, πρέπει στη συνέχεια να αναλυθούν για να προκύψουν κάποια συμπεράσματα. Συχνά απαιτείται συσχέτιση μεταξύ των πληροφοριών από διαφορετικές πηγές, όπως για παράδειγμα, το αρχείο καταγραφής (log file) ενός συστήματος ανίχνευσης εισβολών (Intrusion Detection System) σε ένα δίκτυο μπορεί να συσχετίσει μια ύποπτη δραστηριότητα με έναν υπολογιστή και στη συνέχεια από τα αρχεία καταγραφής του υπολογιστή να προσδιοριστεί ο λογαριασμός του χρήστη και τις ενέργειες που πραγματοποιήθηκαν. Η τακτική παρατήρηση των δραστηριοτήτων των χρηστών κάθε συστήματος και η δημιουργία μιας καθοδηγητικής γραμμής γύρω από την οποία κυμαίνονται οι συνήθεις ενέργειες για κάθε χρήστη, λειτουργούν ως μέτρο σύγκρισης ώστε να ανιχνεύονται ευκολότερα ασυνήθιστες δραστηριότητες.

1.2.4 Αναφορά αποτελεσμάτων

Στη φάση της αναφοράς των αποτελεσμάτων παρουσιάζονται τα συμπεράσματα που προέκυψαν στην προηγούμενη φάση, της ανάλυσης των δεδομένων. Όταν οι πληροφορίες που αφορούν ένα συμβάν δεν είναι πλήρεις και υπάρχουν ανακρίβειες, ίσως να μην είναι δυνατή η διεξαγωγή συμπερασμάτων. Στις περιπτώσεις τις οποίες δυο ή περισσότερα σενάρια είναι πιθανά, αυτά θα πρέπει να αναφέρονται χωριστά και ακολουθώντας μια μεθοδική προσέγγιση θα προτείνεται κάποιο από αυτά ως επικρατέστερο. Τα αποτελέσματα της αναφοράς μπορούν να αποκαλύψουν στο διαχειριστή του συστήματος τις αδυναμίες και τα

ευπαθή σημεία του συστήματος, ώστε να ληφθούν επιπλέον μέτρα προστασίας για το μέλλον.

1.3 Αδρανής Ανάλυση και Ανάλυση πραγματικού χρόνου (Dead and Live Analysis)

Παραδοσιακά, η δικανική υπολογιστών (computer forensics) πραγματοποιούνταν σε ανενεργά συστήματα, δηλαδή σε συστήματα τα οποία βρίσκονταν εκτός λειτουργίας [E113]. Οι ερευνητές απενεργοποιούσαν το υπολογιστικό σύστημα θεωρώντας με αυτό τον τρόπο ότι ασφαλίζουν το σύστημα από οποιαδήποτε επίδραση πάνω στα δεδομένα. Η τοποθέτηση ψηφιακών ωρολογιακών βομβών (digital time-bombs) στο εξεταζόμενο σύστημα από τον επιτιθέμενο, θα μπορούσε να προκαλέσει καταστροφή των δεδομένων [E114]. Οι αναλυτές στη συνέχεια εξέταζαν τα αποθηκευτικά μέσα του συστήματος, όπως για παράδειγμα ένα σκληρό δίσκο, με σχετική ασφάλεια. Αυτού του είδους η ανάλυση ονομάζεται αδρανής ανάλυση (dead analysis) . Τα δεδομένα που μπορούσαν να συλλεχθούν ήταν όλα εκείνα τα οποία είχαν αποθηκευτεί σε κάποιο μέσο (CD, DVD, flash memory, σκληρό δίσκο, χαρτί, κλπ). Ωστόσο τα ίχνη από τις δραστηριότητες του επιτιθέμενου στο σύστημα χάνονταν μαζί με την απενεργοποίηση του συστήματος.

Τα τελευταία χρόνια οι αναλυτές δίνουν έμφαση στην διερεύνηση των συστημάτων σε πραγματικό χρόνο (live analysis) σε ενεργά συστήματα (live system) . Ο λόγος για αυτό είναι ότι οι περισσότερες επιθέσεις που πραγματοποιούνται δεν αφήνουν ίχνη στους σκληρούς δίσκους και στα άλλα αποθηκευτικά μέσα τους συστήματος παρά μόνο στη μνήμη του υπολογιστή. Επίσης, η ευρεία χρήση της κρυπτογραφημένης αποθήκευσης των αρχείων απαιτεί την εύρεση του κλειδιού αποκρυπτογράφησης, ώστε τα αρχεία να είναι αναγνώσιμα. Το μόνο μέρος, που ίσως μπορεί να βρεθεί το κλειδί αποκρυπτογράφησης ενός αρχείου είναι η μνήμη του υπολογιστή. Συνεπώς, η εξέταση ενός συστήματος ενώ αυτό βρίσκεται σε λειτουργία, είναι αναγκαία ώστε να συλλεχθούν όσο το δυνατόν περισσότερα στοιχεία.

1.4 Δικανική Υπολογιστών σε δικτυακό περιβάλλον

Η εφαρμογή της Δικανικής Υπολογιστών σε δικτυακό περιβάλλον (Network Forensics), αναφέρεται στη σύλληψη, καταγραφή και ανάλυση δεδομένων (πακέτων) τα οποία ανταλλάσσονται μεταξύ δικτύων ή ανάμεσα σε υπολογιστές ενός δικτύου [NIS86]. Από την ανάλυση των δεδομένων μπορεί να αποκαλυφθούν επιθέσεις προς το δίκτυο ή κάποιο υπολογιστή του δικτύου, προσπάθειες παραβίασης των δικλίδων ασφαλείας ή ασυνήθιστη δραστηριότητα σε κάποιον υπολογιστή του δικτύου. Έμφαση δίνεται κυρίως στην πρόληψη εισβολών σε ένα σύστημα και σε μικρότερο βαθμό στη ανίχνευση παραβιάσεων. Σε περίπτωση που μια επίθεση πραγματοποιηθεί σε ένα σύστημα είναι εξαιρετικά δύσκολο να αναλυθούν λεπτομερώς οι συνθήκες και ο τρόπος με τον οποίο πραγματοποιήθηκε η επίθεση.

Αρκετοί εισβολείς διαθέτουν την ικανότητα να καλύπτουν τα ίχνη τους και τα αρχεία καταγραφής ενός τείχους προστασίας (firewall) ή ένα σύστημα ανίχνευσης εισβολών (IDS) παρέχουν μάλλον ανεπαρκή στοιχεία για την διεξαγωγή έρευνας. Ένα σύστημα ανίχνευσης εισβολών παρακολουθεί και ελέγχει το δίκτυο για συγκεκριμένα πρότυπα εισβολών και μόλις ανιχνευθεί κάποιο ενεργοποιείται το σύστημα και καταγράφονται οι δραστηριότητες για περαιτέρω ανάλυση, ειδοποιείται ο διαχειριστής του συστήματος και ίσως διακοπεί η σύνδεση μέσω του τείχους προστασίας. Ωστόσο, αν ο εισβολέας χρησιμοποιήσει κάποια μέθοδο η οποία δεν είναι γνωστή στο σύστημα ανίχνευσης εισβολών (IDS) τότε η εισβολή δεν θα γίνει αντιληπτή από τον ανιχνευτή.

Το πεδίο του “Network Forensics” έρχεται να δώσει λύση στο κενό αυτό. Τα επιπλέον ψηφιακά στοιχεία που απαιτούνται, είναι τα πακέτα δεδομένων που ταξιδεύουν στο δίκτυο. Χρησιμοποιώντας ειδικά προγράμματα που ονομάζονται “packet sniffers” μπορούν να συλλεχθούν πακέτα τα οποία θα είναι χρήσιμα εφόσον μπορούν να διαβαστούν και να υποδείξουν τις ενέργειες του επιτιθέμενου και τις αποκρίσεις του συστήματος που υπέστη την επίθεση. Η ανάλυση των δραστηριοτήτων ενός δικτύου σε πραγματικό χρόνο για την αντιμετώπιση επιθέσεων από επίδοξους εισβολείς και παραβιάσεις του δικτύου, είναι αυτό που χαρακτηρίζει το “Network Forensics”[E12].

1.5 Δεδομένα από αρχεία δεδομένων

Ένα αρχείο δεδομένων (data file) είναι μια συλλογή πληροφοριών, λογικά ομαδοποιημένων σε μια οντότητα, η οποία προσδιορίζεται από ένα μοναδικό όνομα (filename). Ένα αρχείο μπορεί να είναι οποιουδήποτε τύπου δεδομένων ανάμεσα σε πολλούς διαθέσιμους, όπως αρχείο κειμένου, εικόνας, βίντεο ή αρχείο κάποιας εφαρμογής. Η επιτυχία της διαδικασίας διερεύνησης (forensic process) των υπολογιστικών αποθηκευτικών συσκευών εξαρτάται από την ικανότητα συλλογής, εξέτασης και ανάλυσης των αρχείων δεδομένων που βρίσκονται σε αυτά τα αποθηκευτικά μέσα.

1.5.1 Αποθηκευτικά Μέσα

Η ευρεία χρήση υπολογιστών και άλλων ψηφιακών συσκευών έχει ως αποτέλεσμα μια πληθώρα συσκευών αποθήκευσης. Οι σκληροί δίσκοι, οι οπτικοί δίσκοι και η flash memory (USB stick) είναι τα πλέον δημοφιλή αποθηκευτικά μέσα, παρόλα αυτά υπάρχουν πολλά περισσότερα. Στον παρακάτω πίνακα αναφέρονται ενδεικτικά μερικά από αυτά.

Τύπος Μέσου	Τυπική Χωρητικότητα	Σχόλια
Εύκαμπτοι δίσκοι (Floppy disk)	1.44 MB	Δισκέτα 3.5 ιντσών
CD - ROM	650 MB – 900 MB	CD-R(μονή εγγραφή), CD-RW(επανεγγράψημα)
DVD - ROM	4.7 GB – 17.08 GB	Δίσκοι μονής και διπλής στρώσης και όψης
Σκληρός Δίσκος	40 GB – 2 TB	Εσωτερικοί και εξωτερικοί
Zip disk	100 MB – 750 MB	Συναντώνται σπάνια
Jaz disk	1 GB – 2 GB	Δεν κατασκευάζονται πλέον
Μαγνητικές Ταινίες (Magnetic Tapes)	80 MB – 1 TB	Χρήση για αντίγραφα ασφαλείας
Flash drive	512 MB – 64 GB	USB διασύνδεση
Compact flash	512 MB – 100 GB	Χρήση σε ψηφιακές συσκευές
Multimedia Card (MMC)	512 MB – 2 GB	Χρήση σε ψηφιακές συσκευές
Secure Digital Card (SD)	512 MB – 2 GB	Χρήση σε ψηφιακές συσκευές
Memory Stick	2 GB -16 GB	Χρήση σε ψηφιακές συσκευές

Εικόνα 1.2. Αποθηκευτικά Μέσα

1.5.2 Συστήματα Αρχείων (Filesystem)

Για να μπορέσει ένα αποθηκευτικό μέσο να χρησιμοποιηθεί για την φύλαξη δεδομένων πρέπει πρώτα να διαμορφωθεί (formatted) και να χωριστεί (partitioning) σε λογικά μέρη ή τόμους (logical volumes). Ο διαχωρισμός ενός μέσου αναφέρεται στην λογική διαίρεση του μέσου σε ανεξάρτητα τμήματα τα οποία λειτουργούν σαν να πρόκειται για φυσικά ανεξάρτητες συσκευές. Ένας λογικός τόμος (logical volume) αποτελείται από ένα ή περισσότερα τμήματα (partitions) ενός αποθηκευτικού μέσου τα οποία έχουν διαμορφωθεί με ένα κοινό σύστημα αρχείων (file system). Η διαμόρφωση ενός λογικού τόμου εξαρτάται από το εκάστοτε σύστημα αρχείων (file system). Το σύστημα αρχείων προσδιορίζει τον τρόπο με τον οποίο τα αρχεία ονομάζονται, αποθηκεύονται, οργανώνονται και προσπελάζονται στους λογικούς τόμους. Υπάρχουν πολλά διαθέσιμα συστήματα αρχείων, καθένα με ξεχωριστά χαρακτηριστικά και διαφορετικού τρόπους οργάνωσης των δεδομένων, παρόλα αυτά υπάρχουν κάποια γνωρίσματα τα οποία είναι κοινά στα περισσότερα από αυτά. Οι κατάλογοι (directories) είναι δομές οργάνωσης που χρησιμεύουν για την ομαδοποίηση των αρχείων. Κάθε κατάλογος μπορεί να περιέχει άλλους καταλόγους οι οποίοι ονομάζονται υποκατάλογοι (subdirectories) για καλύτερη οργάνωση των αρχείων(files). Επίσης τα συστήματα αρχείων χρησιμοποιούν κάποια δομή δεδομένων ώστε να προσδιορίζουν τη θέση του κάθε αρχείου στο αποθηκευτικό μέσο.

Οι τύποι συστημάτων αρχείων κατηγοριοποιούνται σε συστήματα αρχείων δίσκων (disk file systems), συστήματα αρχείων δικτύων (network file systems) και συστήματα αρχείων ειδικής χρήσης (special purpose file systems).

Τα συστήματα αρχείων δίσκων χρησιμοποιούνται συνήθως για την αποθήκευση αρχείων σε σκληρούς δίσκους. Παραδείγματα συστημάτων αρχείων δίσκων αποτελούν τα FAT (FAT12, FAT16, FAT32, exFAT), NTFS, HFS, HFS+, HPFS, ext2, ext3, ext4, ReiserFS, UFS, ISO 9660, ODS-5, ZFS και τα UDF (χρησιμοποιείται στα DVD), CDFS (χρησιμοποιείται στα CD). Τα συστήματα αρχείων δικτύων λειτουργούν ως πελάτες (clients) για ένα απομακρυσμένο πρωτόκολλο πρόσβασης αρχείων (file access protocol) παρέχοντας πρόσβαση στα αρχεία ενός εξυπηρετητή (server). Παραδείγματα συστημάτων αρχείων δικτύων είναι τα NFS, AFS, SMB. Τα συστήματα αρχείων ειδικής χρήσης

περιλαμβάνουν όλα τα υπόλοιπα συστήματα αρχείων που δεν περιλαμβάνονται στις δυο προηγούμενες κατηγορίες.

Όπως αναφέρθηκε προηγουμένως, τα συστήματα αρχείων χρησιμοποιούνται για την αποθήκευση αρχείων στα αποθηκευτικά μέσα. Ωστόσο τα συστήματα αρχείων μπορεί επίσης να κρατούν επιπλέον πληροφορίες από διαγραμμένα αρχεία ή από υπολείμματα διαγραμμένων αρχείων (data fragments). Όταν ένα αρχείο διαγράφεται στην πραγματικότητα δεν διαγράφεται από το αποθηκευτικό μέσο αλλά η πληροφορία της δομής του καταλόγου (directory), στο οποίο βρίσκεται το αρχείο και η οποία δείχνει τη θέση του αρχείου μέσα στο μέσο, αλλάζει σε διαγραμμένο. Το λειτουργικό σύστημα θεωρεί τον χώρο που καταλαμβάνει το αρχείο ως ελεύθερο (παρόλο που αυτό εξακολουθεί να βρίσκεται στο μέσο) και μπορεί να γράψει σε αυτόν οποιοδήποτε άλλο αρχείο μικρότερου ή ίσο μεγέθους με αυτό που διαγράφηκε. Η μικρότερη αποθηκευτική μονάδα που μπορεί να διαχειριστεί ένα σύστημα αρχείων είναι το cluster (αναφέρεται και ως file allocation unit) και το οποίο έχει σταθερό μέγεθος ανεξάρτητα από το μέγεθος κάθε αρχείου. Στην περίπτωση ενός αρχείου με μέγεθος μικρότερο του ενός cluster, δεσμεύεται υποχρεωτικά το μέγεθος ολόκληρου του cluster και εγγράφεται σε αυτό το αρχείο. Ο υπόλοιπος χώρος εντός του cluster που περίσσεψε εξακολουθεί να περιέχει τις πληροφορίες από το αρχείο που υπήρχε προηγουμένως. Το ίδιο ισχύει και σε αρχεία που απαιτούν περισσότερα clusters, καθώς το τελευταίο από τα clusters που δεσμεύει το αρχείο δεν θα είναι τελείως γεμάτο (το αντίθετο συμβαίνει σπάνια) και θα περιέχει χρήσιμες πληροφορίες για το προηγούμενα αποθηκευμένο αρχείο. Αυτός ο αχρησιμοποίητος χώρος ονομάζεται slack space.

1.5.3 Συλλογή των Δεδομένων από τα Αρχεία Δεδομένων

Κατά την διάρκεια της συλλογής των δεδομένων, θα πρέπει να δημιουργηθούν αντίγραφα των προς εξέταση αρχείων. Η δημιουργία ενός κύριου αντιγράφου, το οποίο θα χρησιμοποιείται για την δημιουργία περαιτέρω αντιγράφων, είναι απαραίτητη. Οποιαδήποτε ενέργεια θα γίνεται στα επιπλέον αντίγραφα που δημιουργήθηκαν, ενώ το κύριο αντίγραφο θα παραμένει ανέπαφο και θα χρησιμοποιείται μόνο για τη δημιουργία επιπλέον αντιγράφων. Είναι σημαντικό

κατά την συλλογή των δεδομένων να μην αλλάζουν οι χαρακτηριστικές ιδιότητες των αρχείων όπως αυτή της χρονοσφραγίδας (timestamp) η οποία δείχνει χρήσιμες χρονικές πληροφορίες όπως την τελευταία τροποποίηση ή πρόσβαση στο αρχείο.

Τα δεδομένα μπορούν να αντιγραφούν από ένα αποθηκευτικό μέσο με τη χρήση δυο διαφορετικών τεχνικών:

- **Λογική Αντιγραφή** (Logical Backup): Η δημιουργία λογικού αντιγράφου, αντιγράφει τους καταλόγους και τα αρχεία από μία λογική μονάδα (logical volume), δεν αντιγράφει όμως δεδομένα που μπορεί να βρίσκονται στο αποθηκευτικό μέσο υπό την μορφή διαγραμμένων αρχείων ή δεδομένων που βρίσκονται στο slack space.

- **Bit προς Bit Αντιγραφή** (Bit Stream Imaging): Αυτή η τεχνική είναι επίσης γνωστή και ως disk imaging και δημιουργεί ακριβή αντίγραφα όλων των περιοχών του αποθηκευτικού μέσου [E15]. Επειδή πρωτίστως ενδιαφέρει η ακρίβεια του αντιγράφου σε σχέση με το πρωτότυπο, η εγκυρότητα της διαδικασίας αντιγραφής βασίζεται σε έναν μαθηματικό υπολογισμό του CRC (Cyclic Redundancy Check). Υπολογίζεται αρχικά το CRC της αρχικής πηγής των δεδομένων και έπειτα αυτό του αντιγράφου για να γίνει σύγκριση [E17].

Όταν πρόκειται για περιπτώσεις ηλεκτρονικού εγκλήματος η ακρίβεια των αντιγράφων είναι εξαιρετικά σημαντική καθώς τα ηλεκτρονικά στοιχεία πρέπει να παραμείνουν αναλλοίωτα. Η Bit προς Bit αντιγραφή διατηρεί αυτά τα στοιχεία αλλά απαιτεί περισσότερο αποθηκευτικό χώρο και χρειάζεται περισσότερο χρόνο για να ολοκληρωθεί. Με την τεχνική της Bit προς Bit αντιγραφής υπάρχει η δυνατότητα είτε ενός disk-to-disk αντιγράφου είτε ενός disk-to-file αντιγράφου. Η πρώτη περίπτωση αντιγραφής, αντιγράφει τα περιεχόμενα του αποθηκευτικού μέσου σε ένα άλλο παρόμοιο μέσο, το οποίο πρέπει πρώτα να έχει καθαριστεί από κάθε ίχνος προηγούμενων δεδομένων. Το πλεονέκτημα αυτής της μεθόδου είναι ότι το αντίγραφο μπορεί να συνδεθεί κατευθείαν με έναν υπολογιστή και τα περιεχόμενα του να γίνουν άμεσα διαθέσιμα. Η περίπτωση του disk-to-file αντιγράφου, αντιγράφει τα περιεχόμενα του αποθηκευτικού μέσου σε ένα λογικό αρχείο

δεδομένων (data file image). Το αρχείο αυτό (disk image) περιέχει ακριβώς τα δεδομένα και τη δομή που αυτά είχαν στο αρχικό μέσο, τον ελεύθερο χώρο (free space) και το slack space. Με αυτή τη μέθοδο το αρχείο μπορεί να μετακινηθεί και να αντιγραφεί εύκολα. Ωστόσο για να μπορέσει κάποιος να αναγνώσει τα περιεχόμενα ενός τέτοιου αρχείου θα πρέπει να το επαναφέρει στην αρχική του μορφή (καθώς πρόκειται για συμπιεσμένη μορφή αρχείου) μεταφέροντας το σε κάποιο φυσικό αποθηκευτικό μέσο. Εναλλακτικά η ανάγνωση ενός τέτοιου αρχείου μπορεί να γίνει χρησιμοποιώντας κάποιο ειδικό πρόγραμμα το οποίο μπορεί να αναπαραστήσει τα λογικά περιεχόμενα εικονικών αρχείων (bit stream images). Εργαλεία τα οποία πραγματοποιούν Bit προς Bit αντιγραφή δεν θα πρέπει να χρησιμοποιούνται σε ενεργά συστήματα (live system) για τη δημιουργία αντιγράφων ολόκληρων φυσικών συσκευών καθώς τα αρχεία σε ένα ενεργό συστήματα συνεχώς μεταβάλλονται.

Η διαδικασία δημιουργίας αντιγράφων είναι σημαντική γιατί τα αντίγραφα πρέπει να είναι πανομοιότυπα με τα πρωτότυπα αλλά είναι επίσης σημαντικό να εξασφαλιστεί η ακεραιότητα των δεδομένων του αρχικού μέσου κατά την διάρκεια της αντιγραφής. Ειδικά εργαλεία (write-blocker) χρησιμοποιούνται για εξασφαλιστεί ότι δεν θα αλλάξουν τα δεδομένα στο αρχικό μέσο. Ένα τέτοιο εργαλείο εμποδίζει τον υπολογιστή να πραγματοποιήσει οποιαδήποτε εγγραφή στο αποθηκευτικό μέσο που είναι συνδεδεμένο με αυτόν και μπορεί να είναι είτε κάποια συσκευή (hardware) είτε κάποιο λογισμικό (software). Ένας software write-blocker φιλτράρει τα σήματα διακοπών (interrupts) που στέλνονται στο αποθηκευτικό μέσο ώστε να μπλοκάρει αυτά που θα προκαλέσουν εγγραφή στο μέσο. Το λογισμικό εγκαθίσταται στον υπολογιστή προτού συνδεθεί σε αυτόν η συσκευή που πρέπει να προστατευθεί. Οι συσκευές (hardware) write-blocker συνδέονται ανάμεσα στο αποθηκευτικό μέσο και το υπολογιστικό σύστημα ώστε να εμποδίσουν οποιαδήποτε απόπειρα εγγραφής σε αυτό. Μετά την πραγματοποίηση του αντιγράφου πρέπει να επαληθευτεί η ακεραιότητα του. Πέρα από τον υπολογισμό του CRC (το αποτέλεσμα του οποίου μπορεί να είναι παραπλανητικό σε περιπτώσεις σκόπιμης τροποποίησης των δεδομένων), χρησιμοποιείται η σύνοψη μηνύματος (message digest). Η σύνοψη μηνύματος προκύπτει έπειτα από την εφαρμογή κάποιου κρυπτογραφικού αλγόριθμου κατατεμαχισμού (cryptographic hash function), όπως ο MD5 και ο SHA-1, παρέχοντας μεγαλύτερη ασφάλεια

καθώς είναι σχεδόν αδύνατο να παραποιηθούν τα δεδομένα και ταυτόχρονα να προκύψει η ίδια σύνοψη μηνύματος [E16].

1.5.4 Πληροφορίες Χρονοσφραγίδας

Τα περισσότερα λειτουργικά συστήματα καταγράφουν χρονικές πληροφορίες που σχετίζονται με συγκεκριμένες ενέργειες προς τα αρχεία, τις λεγόμενες πληροφορίες χρονοσφραγίδας (timestamp). Οι πιο συνηθισμένες ενέργειες που καταγράφονται από τα περισσότερα λειτουργικά συστήματα είναι οι χρόνοι που αφορούν το χρόνο δημιουργίας του αρχείου (creation time), τελευταίας τροποποίησης (modification time) του αρχείου και το χρόνο τελευταίας προσπέλασης (access time).

- **Χρόνος Προσπέλασης**: Αφορά την τελευταία χρονική στιγμή που πραγματοποιήθηκε οποιαδήποτε ενέργεια προσπέλασης προς το αρχείο, όπως άνοιγμα του αρχείου, ανάγνωση ή εκτύπωση του αρχείου.

- **Χρόνος Τροποποίησης**: Αφορά την τελευταία χρονική στιγμή που πραγματοποιήθηκε οποιαδήποτε ενέργεια η οποία τροποποίησε το αρχείο.

- **Χρόνος Δημιουργίας**: Αφορά την χρονική στιγμή που δημιουργήθηκε το αρχείο. Όταν ένα αρχείο αντιγράφεται σε ένα σύστημα, ο χρόνος δημιουργίας είναι η στιγμή κατά την οποία το αρχείο αντιγράφεται στο νέο σύστημα.

Σε συστήματα UNIX καταγράφεται και ο χρόνος της τελευταίας αλλαγής του i-node. Το i-node περιλαμβάνει ένα σύνολο χαρακτηριστικών του αρχείου, όπως τα δικαιώματα που έχουν οι διάφοροι χρήστες στο αρχείο. Επίσης ορισμένα συστήματα UNIX κρατούν και το χρόνο τελευταίας τροποποίησης των μεταδεδομένων (metadata) του αρχείου. Τα μεταδεδομένα παρέχουν δεδομένα για τα δεδομένα [E18]. Περιέχουν χαρακτηριστικά του αρχείου (όνομα, μέγεθος, τύπος δεδομένων κλπ.), πληροφορίες που αφορούν τη δομή των δεδομένων (μήκος, πλήθος πεδίων και στηλών κλπ.), συσχετίσεις με άλλα αρχεία, την

ποιότητα των δεδομένων και άλλα στοιχεία που ποικίλουν ανάλογα με τον τύπο των δεδομένων.

Η διατήρηση των χρονικών πληροφοριών που υπάρχουν στα αρχεία θα πρέπει να διατηρηθούν αναλλοίωτες ώστε να προκύψει ένα ακριβές χρονοδιάγραμμα των γεγονότων που συνέβησαν. Η Bit προς Bit αντιγραφή δεν αλλάζει αυτούς τους χρόνους, ωστόσο υπάρχουν κάποιοι άλλοι λόγοι για τους οποίους οι χρονικές πληροφορίες μπορεί να μην είναι ακριβείς ή με αρκετή λεπτομέρεια.

- Το ρολόι του υπολογιστή δεν δείχνει απαραίτητα την σωστή ώρα καθώς μπορεί να μην έχει ρυθμιστεί σωστά ή να έχει μια αυθαίρετη τιμή.

- Σε συστήματα τα οποία έχουν παραβιαστεί μπορεί ο επιτιθέμενος να έχει τροποποιήσει τις χρονικές πληροφορίες κάποιων αρχείων.

1.5.5 Τεχνικά ζητήματα

Κατά την διάρκεια συλλογής των δεδομένων από τα διάφορα αποθηκευτικά μέσα, διάφορες δυσκολίες θα παρουσιαστούν, οι οποίες θα καθυστερήσουν ή θα αποτρέψουν την συλλογή των δεδομένων. Ειδικά εργαλεία και τεχνικές (anti-forensics) χρησιμοποιούνται, ώστε ο επιτιθέμενος να εξαφανίσει τα ψηφιακά ίχνη που άφησε και τα οποία θα προδώσουν τις δραστηριότητες του.

Το πρώτο ζητούμενο είναι η απόκτηση των διαγραμμένων αρχείων και των υπολειμμάτων αρχείων που βρίσκονται στον ελεύθερο χώρο του μέσου και στο slack space. Η τεχνική του “σκουπίσματος” (wiping) χρησιμοποιείται για να παρεμποδιστεί η συλλογή τέτοιων δεδομένων, η οποία επανεγγράφει σε αρχεία ή σε ολόκληρο το μέσο μια τυχαία ακολουθία από 0 και 1 ώστε να επεγγραφούν (overwrite) στα υπάρχοντα δεδομένα. Η επαναλαμβανόμενη εφαρμογή της τεχνικής αυτής αυξάνει την καταστροφική της ισχύ. Ένας άλλος τρόπος ο οποίος μπορεί να δυσχεράνει την συλλογή των δεδομένων ή ακόμα και να καταστήσει αδύνατη την επαναφορά τους, είναι ο απομαγνητισμός (degaussing) του μέσου.

Ένα δεύτερο ζητούμενο είναι η συλλογή των κρυφών δεδομένων. Τα περισσότερα λειτουργικά συστήματα δίνουν τη δυνατότητα στο χρήστη να σημειώσει κάποια

αρχεία, καταλόγους ή ακόμα και ολόκληρα διαμερίσματα (partitions) του μέσου ως κρυφά (hidden). Τα κρυφά αρχεία δεν εμφανίζονται στη λίστα με τα περιεχόμενα ενός καταλόγου και επομένως δεν γίνονται αμέσως αντιληπτά. Μερικές εφαρμογές αλλά και λειτουργικά συστήματα, κρύβουν κάποια από τα αρχεία τους ώστε να μην είναι ορατά από το χρήστη, μειώνοντας την πιθανότητα διαγραφής ή τροποποίησης τους από λάθος του χρήστη. Ένα κρυφό διαμέρισμα μπορεί να περιέχει κάποιο άλλο λειτουργικό σύστημα ή αρχεία δεδομένων. Οι περισσότεροι σκληροί δίσκοι έχουν κάποιες ειδικές περιοχές, όπως τη λεγόμενη HPA (Host Protected Area) και την DCO (Device Configuration Overlay), οι οποίες βρίσκονται στο τέλος του δίσκου και προορίζονται για χρήση μόνο από τον κατασκευαστή [MAY06, E19]. Αυτές οι περιοχές περιέχουν πληροφορίες και διάφορα εργαλεία τοποθετημένα από τον εκάστοτε κατασκευαστή και σχεδιάστηκαν ώστε να μην είναι εύκολη η τροποποίηση , η διαγραφή και η πρόσβαση τους από το χρήστη, το BIOS ή το λειτουργικό σύστημα. Ωστόσο με ειδικά εργαλεία είναι δυνατή η τροποποίηση αυτών των περιοχών και η τοποθέτηση άλλων δεδομένων.

Σε μερικές περιπτώσεις τα δεδομένα ενός μόνο αρχείου δεν βρίσκονται σε ένα αποθηκευτικό μέσο αλλά είναι κατανεμημένα σε περισσότερα, ξεχωριστά μέσα. Μια τέτοια περίπτωση είναι οι συστοιχίες RAID που χρησιμοποιούν την τεχνική striping (όπως η RAID-0 και η RAID-5) για καλύτερη απόδοση [E110]. Σε μια τέτοια συστοιχία σκληρών δίσκων, ισομεγέθη διαμερίσματα στους δίσκους περιέχουν τα δεδομένα ομοιόμορφα κατανεμημένα σε όλα τα διαμερίσματα που ανήκουν στην ίδια λογική μονάδα (volume). Σε αυτή την περίπτωση απαιτούνται όλοι οι δίσκοι οι οποίοι απαρτίζουν τη συστοιχία ώστε να δημιουργηθούν αντίγραφα των δίσκων, η συστοιχία να ξαναδημιουργηθεί σε κάποιο άλλο σύστημα και στη συνέχεια να συλλεχθούν τα δεδομένα.

1.5.6 Εξέταση των Αρχείων Δεδομένων

Μετά την δημιουργία αντιγράφων από τα διάφορα αποθηκευτικά μέσα, τα αντίγραφα μπορούν πλέον να εξεταστούν. Τα δεδομένα των αντιγράφων πρέπει να παραμείνουν ανέπαφα και αναλλοίωτα, σαν να πρόκειται για τα γνήσια αποθηκευτικά μέσα για αυτό θα πρέπει να προσπελαύνονται μόνο για ανάγνωση (read only) ώστε να διασφαλιστεί η ακεραιότητα τους.

Η εικόνα ενός δίσκου (disk image) μπορεί να περιέχει πολύ μεγάλο όγκο δεδομένων καθώς περιέχει και τον ελεύθερο χώρο του δίσκου αλλά και το slack space, τα οποία με τη σειρά τους μπορεί να περιέχουν χιλιάδες αρχεία ή τμήματα αρχείων. Τα δεδομένα αυτά πρέπει να εξαχθούν και η διαδικασία ίσως να γίνει περισσότερο πολύπλοκη αν προστατεύονται από κωδικούς ή βρίσκονται σε κρυπτογραφημένη μορφή. Με την χρήση διάφορων εργαλείων η διαδικασία εξαγωγής των δεδομένων μετατρέπει τα δεδομένα από τον αχρησιμοποίητο χώρο σε αρχεία δεδομένων, καθώς επίσης επαναφέρει τα διαγραμμένα αρχεία. Η εμφάνιση των περιεχομένων του slack space γίνεται με την χρήση ειδικών προγραμμάτων (hex editors) τα οποία εμφανίζουν τα ακριβή περιεχόμενα ενός αρχείου σε 16-αδική μορφή (raw data) χωρίς να γίνεται συσχέτιση με το τύπο των δεδομένων που περιέχει το αρχείο [E111].

Αφού τα δεδομένα έχουν πλέον εξαχθεί, για να γίνουν κατανοητά τα περιεχόμενα ενός αρχείου είναι απαραίτητη η γνώση του τύπου των δεδομένων που περιέχονται στο αρχείο. Όλα τα αρχεία έχουν μια προέκταση-κατάληξη (εφόσον υποστηρίζεται από το λειτουργικό σύστημα) η οποία υποδηλώνει τον τύπο των δεδομένων του αρχείου. Ωστόσο η κατάληξη ενός αρχείου δεν αποτελεί εγγύηση για τον τύπο των δεδομένων καθώς υπάρχει η δυνατότητα από το χρήστη να αλλάξει την κατάληξη του αρχείου. Ο τύπος του αρχείου μπορεί να αναγνωριστεί από τις πληροφορίες (metadata) που περιέχονται στην κεφαλίδα του αρχείου (file header). Κάθε τύπος δεδομένων φέρει μια συγκεκριμένη υπογραφή από την οποία μπορεί να αναγνωριστεί. Από την κεφαλίδα του αρχείου μπορεί επίσης να αναγνωριστεί αν πρόκειται για κρυπτογραφημένο αρχείο. Ένας άλλος αποτελεσματικός τρόπος αναγνώρισης του τύπου ενός αρχείου, είναι με τη χρήση ιστογράμματος το οποίο απεικονίζει την κατανομή των ASCII τιμών ως ποσοστό του συνόλου των χαρακτήρων του αρχείου. Για παράδειγμα, συχνή εμφάνιση του κενού διαστήματος και φωνηέντων, δείχνουν ότι πρόκειται για αρχείο κειμένου ενώ μια ισορροπημένη κατανομή του ιστογράμματος δείχνει ότι πρόκειται για συμπιεσμένο αρχείο. Με παρόμοιο τρόπο μπορούν να ανιχνευθούν κρυπτογραφημένα αρχεία (encrypted files). Η κεφαλίδα του κρυπτογραφημένου αρχείου μπορεί να υποδείξει τη μέθοδο κρυπτογράφησης που χρησιμοποιήθηκε, η πρόσβαση όμως στα περιεχόμενα τους δεν είναι δυνατή χωρίς την χρήση του κλειδιού αποκρυπτογράφησης. Ενώ η ανίχνευση κρυπτογραφημένων αρχείων

είναι σχετικά εύκολη, η χρήση στεγανογραφίας (steganography) είναι δυσκολότερη να ανιχνευθεί. Στεγανογραφία είναι η εμφώλευση δεδομένων μέσα σε άλλα δεδομένα. Παραδείγματα στεγανογραφίας είναι τα ψηφιακά υδατογραφήματα (digital watermarks) και η χρήση εικόνων οι οποίες περιέχουν κρυμμένα μηνύματα και πληροφορίες.

1.6 Δεδομένα από το Λειτουργικό Σύστημα

Το Λειτουργικό Σύστημα (Operating System) είναι ένα πρόγραμμα το οποίο χειρίζεται τις λεπτομέρειες λειτουργίας των συσκευών ενός υπολογιστή ή κάποιας άλλης ηλεκτρονικής συσκευής. Αποτελεί την πλατφόρμα πάνω στην οποία εκτελούνται οι υπόλοιπες εφαρμογές και είναι υπεύθυνο για τη σωστή διαμοίραση των πόρων του συστήματος. Πέρα από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών (Windows, Linux, UNIX, Mac OS), υπάρχουν και άλλα εξειδικευμένα λειτουργικά συστήματα για κάθε ηλεκτρονική συσκευή. Τα λειτουργικά συστήματα κρατούν πληροφορίες σχεδόν για οτιδήποτε συμβεί σε ένα σύστημα, για αυτό είναι σημαντική η γνώση των δεδομένων που μπορούν να συλλεχθούν από αυτά. Τα δεδομένα ενός λειτουργικού συστήματος μπορεί να βρίσκονται είτε υπό την μορφή μη μεταβλητών (δηλαδή αποθηκευμένων) δεδομένων (non-volatile data), είτε υπό την μορφή προσωρινών δεδομένων (volatile data), τα οποία έχουν να κάνουν με την τρέχουσα κατάσταση του συστήματος [LEB07, E112].

1.6.1 Μη ασταθή δεδομένα του Λειτουργικού Συστήματος

Η κυριότερη πηγή μη μεταβλητών δεδομένων (non volatile data) σε ένα λειτουργικό σύστημα είναι το σύστημα αρχείων (filesystem). Το σύστημα αρχείων παρέχει αποθηκευτικό χώρο στο λειτουργικό σύστημα σε ένα ή περισσότερα μέσα αποθήκευσης [E13]. Υπάρχουν βέβαια περιπτώσεις όπου το σύστημα αρχείων αλλά και ολόκληρο το λειτουργικό σύστημα, βρίσκονται σε κάποιο αφαιρούμενο αποθηκευτικό μέσο και από εκεί φορτώνονται δυναμικά στην μνήμη του συστήματος, με αποτέλεσμα τα δεδομένα τους να είναι ευμετάβλητα (volatile data). Γενικά, οι τύποι των δεδομένων που περιέχονται σε ένα λειτουργικό σύστημα είναι:

- **Αρχεία διαμόρφωσης (Configuration Files):** Τα αρχεία αυτά περιέχουν ρυθμίσεις του λειτουργικού συστήματος και των εφαρμογών, επιλεγμένες από το χρήστη (κάποιες εφαρμογές διατηρούν ξεχωριστά αρχεία διαμόρφωσης από αυτά του λειτουργικού συστήματος). Τα πιο συνηθισμένα είναι τα αρχεία που περιέχουν πληροφορίες για:

  - **Χρήστες και ομάδες χρηστών.** Περιέχει τους λογαριασμούς των χρηστών μαζί με πληροφορίες όπως τα στοιχεία και τα δικαιώματα του κάθε χρήστη.

  - **Αρχεία Κωδικών.** Το λειτουργικό σύστημα αποθηκεύει σε αυτά τα αρχεία κωδικούς σε κατακερματισμένη μορφή (password hashes).

  - **Προγραμματισμένες Εργασίες.** Οι εργασίες αυτές είναι προγραμματισμένες να εκτελούνται αυτόματα σε κάποια καθορισμένη χρονική στιγμή ή περιοδικά, όπως ο έλεγχος για ιούς.

- **Αρχεία Καταγραφής (log files):** Τα αρχεία καταγραφής περιέχουν πληροφορίες σχετικές με διάφορα συμβάντα του λειτουργικού συστήματος καθώς επίσης και συμβάντα που συνέβησαν από εφαρμογές. Τα γεγονότα συνήθως καταγράφονται σε αρχεία κειμένου ή σε ειδικές βάσεις δεδομένων. Οι συνηθέστεροι τύποι πληροφορίας που μπορούν να βρεθούν σε ένα αρχείο καταγραφής είναι:

  - **Συμβάντα Συστήματος.** Πρόκειται για συμβάντα που πραγματοποιήθηκαν από το λειτουργικό σύστημα. Αποτυχημένες ή επιτυχημένες προσπάθειες εκτέλεσης σημαντικών ενεργειών ή ενεργειών που έχει ορίσει ο διαχειριστής του συστήματος είναι ορισμένα από τα συμβάντα που καταγράφονται. Κάθε εγγραφή περιέχει τον κωδικό του συμβάντος, κωδικό σφάλματος και κατάστασης, πληροφορίες χρονοσφραγίδας (timestamp) και άλλες πληροφορίες.

- **Καταγραφές Επιθεώρησης (Audit Records).** Περιέχει πληροφορίες συμβάντων που αφορούν την ασφάλεια του συστήματος, όπως επιτυχημένες ή αποτυχημένες προσπάθειες αυθεντικοποίησης χρηστών.

- **Συμβάντα Εφαρμογών.** Καταγράφονται πληροφορίες που αφορούν την έναρξη, τον τερματισμό και τις ενέργειες που πραγματοποίησε μια εφαρμογή.

- **Αρχεία εναλλαγής (Swap Files).** Πρόκειται για αρχεία τα οποία δημιουργούνται από το λειτουργικό σύστημα (σε συνεργασία με τη μνήμη RAM) και ουσιαστικά επεκτείνουν την διαθέσιμη μνήμη για τις εφαρμογές, χρησιμοποιώντας κάποιο άλλο αποθηκευτικό μέσο, όπως για παράδειγμα ένα σκληρό δίσκο, εναλλάσσοντας δεδομένα μεταξύ δίσκου και μνήμης RAM.

- **Αρχεία Επαναφοράς (Hibernation Files).** Τα αρχεία αυτά δημιουργούνται για να καταγράψουν την τρέχουσα κατάσταση του συστήματος (περιεχόμενα μνήμης και ανοιχτών αρχείων) πριν τον τερματισμό του, έτσι ώστε την επόμενη φορά που θα ξεκινήσει, να επανέλθει στην κατάσταση που βρισκόταν πριν τον τερματισμό.

1.6.2 Ασταθή Δεδομένα του Λειτουργικού Συστήματος

Το λειτουργικό σύστημα φορτώνεται στη μνήμη RAM του συστήματος και από εκεί εκτελείται. Καθώς το λειτουργικό σύστημα βρίσκεται σε λειτουργία, τα περιεχόμενα της μνήμης RAM διαρκώς αλλάζουν. Λόγω της αστάθειας – μεταβλητότητας που παρουσιάζουν αυτά τα δεδομένα (volatile data) η συλλογή τους από τη μνήμη είναι τόσο κρίσιμη, όσο και σημαντική, καθώς μαρτυρούν τις πιο πρόσφατες δραστηριότητες που πραγματοποιήθηκαν στο σύστημα. Το λειτουργικό σύστημα διαχειρίζεται την μνήμη χωρίζοντας την σε μικρά τμήματα, τις σελίδες (pages ή blocks), τις οποίες κατανέμει στις εφαρμογές. Το μέγεθος του τμήματος μνήμης που μπορεί να δοθεί σε μια εφαρμογή ποικίλει ωστόσο υπάρχει μια ελάχιστη και μια μέγιστη τιμή. Το μέγεθος του τμήματος μνήμης θα είναι μεγαλύτερο από αυτό

που χρειάζεται η εφαρμογή και έτσι ένα κομμάτι θα μείνει αχρησιμοποίητο από αυτήν. Αυτό το αχρησιμοποίητο τμήμα της μνήμης (memory slack space) μπορεί να περιέχει εναπομείναντα δεδομένα από προηγούμενη χρήση αυτού του τμήματος μνήμης. Επίσης, οι ελεύθερες σελίδες (free space) της μνήμης, οι οποίες δεν έχουν εκχωρηθεί σε κάποια εφαρμογή μπορεί επίσης να περιέχουν δεδομένα από προηγούμενη χρησιμοποίηση τους.

Οι συνηθέστεροι τύποι πληροφορίας που παρουσιάζουν αστάθεια και εντοπίζονται στα λειτουργικά συστήματα είναι:

- **Διαμόρφωση Δικτύου (Network Configuration):** Λόγω της δυναμικής φύσης που παρουσιάζει η δικτύωση, η τρέχουσα διαμόρφωση δικτύου είναι αυτή από την οποία θα πρέπει να αντλούνται οι πληροφορίες, όπως οι διευθύνσεις IP και οι ενεργές διεπαφές (interfaces).

- **Συνδέσεις Δικτύου:** Το λειτουργικό σύστημα διεκπεραιώνει εισερχόμενες και εξερχόμενες συνδέσεις μεταξύ του συστήματος και άλλων συστημάτων. Για τις εισερχόμενες συνδέσεις προσδιορίζονται οι πόροι που χρησιμοποιούνται, όπως τα κοινά αρχεία και εκτυπωτές, καθώς επίσης παρέχονται από το λειτουργικό σύστημα οι διευθύνσεις και οι θύρες (ports) που χρησιμοποιούνται.

- **Ενεργές Διεργασίες:** Οι ενεργές διεργασίες που εκτελούνται στο σύστημα μπορεί να προέρχονται από το λειτουργικό σύστημα είτε από εφαρμογές του χρήστη. Μια λίστα με τις ενεργές διεργασίες δεν αποκαλύπτει μόνο τα προγράμματα που εκτελούνται αλλά επίσης φανερώνει και εκείνα τα οποία δεν εκτελούνται για κάποιο λόγο (απενεργοποιήθηκαν ή αφαιρέθηκαν από το σύστημα) ενώ θα έπρεπε, όπως αντιικά προγράμματα (antivirus) και τείχος προστασίας (firewall).

- **Ανοιχτά Αρχεία:** Το λειτουργικό σύστημα παρέχει μια λίστα με τα ανοιχτά αρχεία στο σύστημα και τα οποία μπορούν συσχετιστούν με τις ενεργές διεργασίες.

- **Συνόδους Έναρξης (Login Sessions):** Για κάθε χρήστη ο οποίος εισήλθε πρόσφατα στο σύστημα, προηγούμενες επιτυχημένες ή αποτυχημένες προσπάθειες έναρξης συνόδου, το λειτουργικό σύστημα καταγράφει πληροφορίες όπως η στιγμή έναρξης και λήξης της συνόδου. Οι εγγραφές αυτές μπορούν να βοηθήσουν στον προσδιορισμό της χρήσης του συστήματος από κάποιο χρήστη καθώς και να διαπιστωθεί αν ο λογαριασμός κάποιου χρήστη ήταν ενεργός όταν συνέβη ένα γεγονός στο σύστημα.

- **Ώρα Λειτουργικού Συστήματος:** Η ώρα που κρατάει το λειτουργικό σύστημα αποτελεί μια χρήσιμη πληροφορία για το σχηματισμό χρονοδιαγράμματος των γεγονότων που συνέβησαν στο σύστημα ή ακόμη και συσχέτισης γεγονότων ανάμεσα σε διαφορετικά συστήματα. Ωστόσο η ώρα που κρατάει το λειτουργικό σύστημα ίσως να διαφέρει από αυτήν του BIOS.

Τα ασταθή δεδομένα του Λειτουργικού Συστήματος που αφορούν ένα συμβάν, μπορούν να συλλεχθούν μόνο από ένα ενεργό σύστημα (live system) στο οποίο δεν έχει γίνει επανεκκίνηση από τη στιγμή του συμβάντος. Οποιαδήποτε ενέργεια πραγματοποιηθεί στο σύστημα (είτε από το Λειτουργικό Σύστημα είτε από το χρήστη) σχεδόν σίγουρα θα αλλάξει τα ασταθή δεδομένα κατά κάποιο τρόπο. Η απόφαση για το αν θα πρέπει να συλλεχθούν αυτού του είδους τα δεδομένα και για το αν θα προκύψουν χρήσιμες πληροφορίες από αυτά, πρέπει να ληφθεί άμεσα. Τα εργαλεία που θα χρησιμοποιηθούν για τη συλλογή των δεδομένων (forensic tools), θα πρέπει να τοποθετηθούν σε ένα CD-ROM ή ένα USB flash, και από εκεί να εκτελεστούν, προκαλώντας τη μικρότερη δυνατή αναταραχή στο σύστημα.

ΚΕΦΑΛΑΙΟ 2

Network Forensics – Δικανική Δικτύων

2.1 Εισαγωγή στη Δικανική Δικτύων

Παράλληλα με την αύξηση του διαδικτύου, τα ηλεκτρονικά εγκλήματα και οι παραβιάσεις συστημάτων αυξήθηκαν. Το μεγάλο πρόβλημα της ασφάλειας του διαδικτύου οφείλεται στον αρχικό του σχεδιασμό, ο οποίος δεν προέβλεπε την παράμετρο της ασφάλειας, καθώς αρχικός στόχος ήταν η δημιουργία ενός ανοιχτού συστήματος επικοινωνίας. Οι υπάρχουσες μέθοδοι όπως τα αρχεία καταγραφής των εξυπηρετητών (servers), οι εγγραφές των τειχών προστασίας (firewalls) , τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS – Intrusion Detection and Prevention Systems) δεν επαρκούν για την αναγνώριση ενός έμπειρου επιτιθέμενου. Η Δικανική Δικτύων χρησιμοποιώντας εξειδικευμένα εργαλεία σύλληψης της δικτυακής κίνησης και συσχέτισης δεδομένων από διάφορες δικτυακές οντότητες έχει ως στόχο την πλήρη αποκάλυψη του τρόπου επίτευξης μιας εισβολής και την εμφάνιση των αδυναμιών στην ασφάλεια του συστήματος. [Kan06, Kiz05]

Η Δικανική Δικτύων (Network Forensics), αποτελεί μια νέα προσέγγιση για την έρευνα περιστατικών ασφαλείας σε ένα δίκτυο και την άμεση αντίδραση, οδηγώντας σε μεγαλύτερη ασφάλεια του δικτύου [Ren04]. Είναι μια επέκταση στο μοντέλο της δικτυακής ασφάλειας, όπου η έμφαση παραδοσιακά δίνεται στην πρόληψη και σε μικρότερο βαθμό στην ανίχνευση. Η εστίαση γίνεται στη σύλληψη, την καταγραφή και την ανάλυση δικτυακών πακέτων και συμβάντων, για διερευνητικούς σκοπούς. Η Δικανική Δικτύων έρχεται να συμπληρώσει τα κενά που λείπουν και να δώσει τα επιπλέον στοιχεία που απαιτούνται για μια πλήρη διερεύνηση των συνθηκών, κάτω από τις οποίες πραγματοποιήθηκε μια επίθεση.

Ο όρος Δικανική Δικτύων (Network Forensics) χρησιμοποιείται για να περιγράψει την διαδικασία της ανάλυσης πληροφοριών, οι οποίες έχουν συλλεχθεί σε ένα

ενεργό δίκτυο, από διάφορα εργαλεία επιθεώρησης, παρακολούθησης και ανίχνευσης εισβολών, με σκοπό την προστασία [Bri02**,** Cor02**,** Gar01]. Επίσημος ορισμός δεν υπάρχει, ωστόσο το Digital Forensics Research Workshop παρουσιάζει ως ορισμό της *Δικανικής Δικτύων τη χρήση επιστημονικά αποδεδειγμένων τεχνικών, για τη συλλογή, την αναγνώριση, τη συσχέτιση, την ανάλυση και την καταγραφή ψηφιακών αποδεικτικών στοιχείων από πολλαπλές, ενεργές, ψηφιακές πηγές επεξεργασίας και μετάδοσης, για το σκοπό της αποκάλυψης γεγονότων που σχετίζονται με την σκόπιμα σχεδιασμένη, μη εξουσιοδοτημένη δραστηριότητα, με στόχο την διατάραξη, τη διαφθορά και την κατάληψη ενός συστήματος, καθώς και την παροχή πληροφοριών και βοήθειας για τις παραπάνω δραστηριότητες* [Gar01].

Για το σκοπό της Δικανικής Δικτύων, απαιτούνται κάποια εργαλεία, καταρχήν για την σύλληψη της κίνησης του δικτύου. Ως κίνηση του δικτύου εννοείται η μεταφορά δεδομένων μεταξύ δυο υπολογιστών. Τα δεδομένα ενθυλακώνονται σύμφωνα με το μοντέλο διαστρωμάτωσης του TCP/IP (Επίπεδο Εφαρμογής, Επίπεδο Μεταφοράς, Επίπεδο Internet, Επίπεδο Διασύνδεσης Δικτύου), προσθέτοντας κάθε φορά στην κεφαλίδα κάποιες επιπλέον πληροφορίες που αφορούν το πρωτόκολλο που χρησιμοποιείται. Όλα τα επίπεδα παρέχουν σημαντικές πληροφορίες (διευθύνσεις MAC και IP, πόρτες, κλπ.) στις οποίες βασίζεται η ανάλυση της Δικανικής Δικτύων.

2.1.1 Πηγές δεδομένων της δικτυακής κίνησης

Οι κυριότερες πηγές δεδομένων της δικτυακής κίνησης είναι:

1. **Τείχη προστασίας και Δρομολογητές.** Τα τείχη προστασίας (firewalls) και οι δρομολογητές (routers), εξετάζουν τη δικτυακή κίνηση και επιτρέπουν ή απαγορεύουν τη διέλευση της, με βάση ένα σύνολο κανόνων. Στην περίπτωση που απαγορευτεί η διέλευση κάποιου πακέτου, οι συσκευές αυτές καταγράφουν κάποιες βασικές πληροφορίες. Οι πληροφορίες που καταγράφονται τυπικά περιλαμβάνουν ημερομηνία, ώρα, IP διευθύνσεις πηγής και προορισμού, πρωτόκολλο επιπέδου μεταφοράς (TCP, UDP, ICMP), πληροφορίες του πρωτοκόλλου (TCP ή UDP πόρτες, ICMP τύπος

και κωδικός). Τα περιεχόμενα των πακέτων συνήθως δεν καταγράφονται. Μερικά firewalls και routers που πραγματοποιούν μετάφραση των διευθύνσεων του δικτύου (NAT) καταγράφουν επιπλέον πληροφορίες. NAT είναι η διαδικασία αντιστοίχισης των διευθύνσεων ενός δικτύου σε διευθύνσεις ενός άλλου δικτύου, όπως για παράδειγμα η διαφοροποίηση πολλαπλών εσωτερικών διευθύνσεων ενός δικτύου, που αντιστοιχούν σε μια εξωτερική διεύθυνση, χρησιμοποιώντας διαφορετικό αριθμό πόρτας για κάθε εσωτερική διεύθυνση. Επίσης ορισμένα firewalls λειτουργούν ως ενδιάμεσοι εξυπηρετητές (proxy servers), δεχόμενοι ένα αίτημα από κάποιον υπολογιστή (client) το οποίο αποστέλλουν στον επιθυμητό προορισμό εκ μέρους του client. Έτσι στην πραγματικότητα δημιουργούνται δυο ξεχωριστές συνδέσεις, για τις οποίες επιπλέον πληροφορίες καταγράφονται.

2. **Packet Sniffers και Protocol Analyzers.** Ο Packet Sniffer χρησιμοποιείται για την παρακολούθηση της κίνησης του δικτύου (ενσύρματο ή ασύρματο) και για την καταγραφή των πακέτων που διέρχονται μέσα από αυτό. Μια κάρτα δικτύου NIC, κανονικά δέχεται μόνο πακέτα που προορίζονται για αυτήν, απορρίπτοντας τα υπόλοιπα. Ωστόσο, θέτοντας την κάρτα δικτύου να λειτουργεί σε μια ειδική κατάσταση, το λεγόμενο promiscuous mode, τότε αυτή αποδέχεται όλα τα εισερχόμενα πακέτα, ανεξαρτήτως προορισμού. Σε αυτή τη λειτουργία βασίζονται οι Packet Sniffers, για να καταγράψουν όλα τα πακέτα που περνούν ή εκείνα με κάποια συγκεκριμένα χαρακτηριστικά. Οι περισσότεροι Packet Sniffers λειτουργούν και ως Protocol Analyzers, μπορούν δηλαδή να συναρμολογήσουν τις ροές δεδομένων από τα πακέτα. Πέρα από την ικανότητα να επεξεργάζονται πακέτα κατευθείαν από το δίκτυο (live network traffic), οι Protocol Analyzers μπορούν να επεξεργαστούν και πακέτα από αρχεία, τα οποία έχουν νωρίτερα καταγραφεί από ένα Packet Sniffer. Εξαιρετικά πολύτιμη είναι η ικανότητα των Protocol Analyzers να εμφανίζουν ακατέργαστα τα δεδομένα ενός πακέτου (raw data), σε μη κατανοητή μορφή.

3. **Συστήματα Ανίχνευσης Εισβολών.** Ένα σύστημα ανίχνευσης εισβολών (IDS) παρακολουθεί τα συμβάντα που πραγματοποιούνται σε ένα υπολογιστικό σύστημα ή δίκτυο και τα αναλύει προσπαθώντας να εντοπίσει σημάδια που συνιστούν παραβίαση των κανονισμών ασφαλείας. Υπάρχουν δυο ειδών IDS συστήματα, τα Host IDS, τα οποία παρακολουθούν την κίνηση και τα γεγονότα που συμβαίνουν σε ένα συγκεκριμένο υπολογιστή και τα Network IDS, τα οποία παρακολουθούν την κίνηση ολόκληρου του δικτύου ή τμήματος αυτού. Σε κάθε περίπτωση τα IDS καταγράφουν τις ίδιες περίπου πληροφορίες με τα firewalls καθώς και ειδικές πληροφορίες που σχετίζονται με την εφαρμογή. Στην περίπτωση που ανιχνευτεί κάποιο ύποπτο συμβάν τα περισσότερα IDS έχουν τη δυνατότητα εκτεταμένης καταγραφής πληροφοριών. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για να συσχετιστούν με τις πληροφορίες από άλλες πηγές ώστε να επιβεβαιωθεί η εγκυρότητα των προειδοποιήσεων (alerts) του IDS. Για την ανίχνευση ύποπτης δραστηριότητας, τα IDS χρησιμοποιούν μία ή συνδυασμό περισσοτέρων από τις εξής τρείς τεχνικές [NIS94]:

   i. Ανίχνευση με βάση την υπογραφή (Signature based Detection). Συγκρίνονται γνωστές υπογραφές με αυτές των συμβάντων, για να αναγνωριστεί κάποιο ύποπτο συμβάν. Η τεχνική είναι πολύ αποτελεσματική στην αναγνώριση γνωστών απειλών αλλά αναποτελεσματική σε νέες-άγνωστες απειλές .

   ii. Ανίχνευση ανωμαλιών (Anomaly-based). Παρατηρώντας για ένα χρονικό διάστημα τις δραστηριότητες και τη συμπεριφορά του δικτύου (ή ενός υπολογιστή), δημιουργείται ένα προφίλ το οποίο αντικατοπτρίζει τη φυσιολογική συμπεριφορά. Συγκρίνοντας το προφίλ της φυσιολογικής συμπεριφοράς με αυτή ενός συμβάντος προσδιορίζεται αν πρόκειται για απειλή ή όχι.

iii. Stateful Protocol Analysis. Βασίζεται σε προτεινόμενα προφίλ του κατασκευαστή, τα οποία προσδιορίζουν τη σωστή χρήση συγκεκριμένων πρωτοκόλλων.

4. **Εξυπηρετητές απομακρυσμένης πρόσβασης.** Οι εξυπηρετητές απομακρυσμένης πρόσβασης (remote access servers) είναι συσκευές όπως οι VPN πύλες (gateways) και οι modem servers, οι οποίες διευκολύνουν τις συνδέσεις μεταξύ δικτύων. Αυτές οι συσκευές καταγράφουν την προέλευση της κάθε σύνδεσης και μπορούν να υποδείξουν το λογαριασμό του χρήστη που πραγματοποίησε τη σύνοδο (session). Οι εξυπηρετητές απομακρυσμένης πρόσβασης λειτουργούν στο επίπεδο δικτύου και για αυτό δεν καταγράφουν πληροφορίες που σχετίζονται με την εφαρμογή.

5. **Λογισμικό διαχείρισης συμβάντων ασφαλείας.** Το λογισμικό διαχείρισης συμβάντων ασφαλείας (SEM – Security Event Management) εισάγει πληροφορίες από διάφορες δικτυακές πηγές (όπως αυτές που αναφέρονται παραπάνω) και συσχετίζει τα συμβάντα που καταγράφηκαν. Δέχεται αντίγραφα των αρχείων καταγραφής (log files) και κανονικοποιεί τα δεδομένα σε μια στάνταρ μορφή.

6. **Εργαλεία Ανάλυσης Δικανικής Δικτύων.** Πρόκειται για εργαλεία γνωστά ως NFAT (Network Forensics Analysis Tools), τα οποία έχουν όλες τις λειτουργίες των Packet Sniffers, των Protocol Analyzers και των προϊόντων SEM μαζί. Τα εργαλεία NFAT επικεντρώνονται στο να συλλέγουν, να εξετάζουν και να αναλύσουν τη δικτυακή κίνηση. Έχουν τη δυνατότητα να ανακατασκευάσουν ένα συμβάν βασιζόμενα στη δικτυακή κίνηση, να οπτικοποιήσουν τη ροή των δεδομένων του δικτύου και να κατασκευάσουν προφίλ φυσιολογικής δραστηριότητας ώστε να αναγνωρίζουν τις σημαντικές αποκλίσεις των δραστηριοτήτων.

2.1.2 Παρακολούθηση και καταγραφή της κίνησης του δικτύου

Η ικανότητα της σύλληψης και της παρακολούθησης της δικτυακής κίνησης είναι βασική προϋπόθεση της καλής διαχείρισης του συστήματος. Η παρακολούθηση της δραστηριότητας του δικτύου δίνει τη δυνατότητα προσδιορισμού της συμπεριφοράς και της αλληλεπίδρασης των εξωτερικών ή εσωτερικών κόμβων με το σύστημα. Κατά τη σύλληψη της κίνησης του δικτύου δεν καταγράφονται πάντα οι ίδιες πληροφορίες για τα πακέτα, καθώς μπορεί να επιλεχθεί να γίνεται καταγραφή ολόκληρων των πακέτων (πληροφορίες κεφαλίδας και τα δεδομένα που μεταφέρει), μόνο των κεφαλίδων ή να συγκεντρωθούν οι πληροφορίες κεφαλίδας από διάφορα πακέτα και να γίνει καταγραφή της ροής (flow record). Η ροή δηλαδή περιλαμβάνει τη σύνοψη πληροφοριών μιας μονοκατευθυντικής επικοινωνίας μεταξύ δυο υπολογιστών. Οι πληροφορίες που καταγράφονται περιλαμβάνουν τις διευθύνσεις προέλευσης-προορισμού, τις πόρτες των πρωτοκόλλων TCP και UDP, τύπο και κωδικό μηνύματος για το ICMP πρωτόκολλο, σήματα (flags) για το TCP πρωτόκολλο, ώρα έναρξης της ροής και διάρκεια, ο όγκος της ροής σε πακέτα και bytes, καθώς και πληροφορίες δρομολόγησης. Η καταγραφή της ροής ξεκινάει όταν πραγματοποιηθεί μια νέα σύνδεση και τερματίζεται είτε όταν η σύνδεση μείνει ανενεργή για ένα διάστημα, είτε όταν τερματιστεί η σύνδεση από το κάποιο σήμα (FIN ή RST). Επίσης είναι πιθανή η διακοπή της καταγραφής της ροής, αν εξαντληθεί ο αποθηκευτικός χώρος της συσκευή καταγραφής. Από την άλλη, υπάρχουν περιπτώσεις όπου η καταγραφή ολόκληρου του πακέτου είναι αναγκαία. Στην περίπτωση που η πλήρης καταγραφή των πακέτων θα ήταν νόμιμη και δεν θα υπήρχε κρυπτογράφηση των δεδομένων ώστε να εμποδίσουν την ανάλυση, η ιδανική λύση θα ήταν η ανάλυση των πληροφοριών της ροής σε πραγματικό χρόνο και η βραχυπρόθεσμη καταγραφή ολόκληρων των πακέτων[McH08].

Η επιλογή της τεχνικής με την οποία θα συλλέγονται οι πληροφορίες από τα πακέτα, εξαρτάται άμεσα από τους εξής παράγοντες:

1. Αποθηκευτική ικανότητα. Η πλήρης καταγραφή της κεφαλίδας και των δεδομένων του πακέτου, απαιτεί πολύ μεγαλύτερο χώρο από ότι μόνο η καταγραφή της κεφαλίδας.

2. Προσωπικά δεδομένα. Οι χρήστες ενός δικτύου μπορεί να δεχτούν να παρακολουθούνται και να καταγράφονται οι πληροφορίες κεφαλίδας. Ωστόσο η παρακολούθηση και καταγραφή των δεδομένων που περιέχονται στα πακέτα, μπορεί να θεωρηθούν ως προσωπικά δεδομένα και η καταγραφή τους να θεωρηθεί παραβίαση της ιδιωτικότητας.
3. Κρυπτογράφηση. Στην περίπτωση που τα δεδομένα που μεταφέρονται στο πακέτο είναι κρυπτογραφημένα, η καταγραφή τους έχει μικρή αξία.

2.2 Διαφοροποίηση από το Computer Forensics

Συχνά ο διαχειριστής ενός δικτύου θα ανακαλύψει στοιχεία τα οποία θα υποδεικνύουν ότι ένας υπολογιστής (host) ο οποίος έχει εκτεθεί σε κάποια επίθεση, δεν αποτελεί μεμονωμένο περιστατικό άλλα αποτελεί τμήμα ενός γενικότερου προβλήματος. Κάπου εδώ η Δικανική Υπολογιστών έρχεται να συναντήσει τη Δικανική Δικτύων.

Λόγω της πολυπλοκότητας των δικτύων και της πληθώρας δικτυακών συσκευών που το απαρτίζουν, η Δικανική Δικτύων είναι δυσκολότερο να πραγματοποιηθεί. Καταρχήν, ο όγκος των δεδομένων προς συλλογή και ανάλυση, είναι σημαντικά μικρότερος στην περίπτωση ενός μεμονωμένου υπολογιστή από ότι σε ένα δίκτυο. Όταν εξετάζεται ένας μεμονωμένος υπολογιστής, μπορούν να δημιουργηθούν πλήρη αντίγραφα των δίσκων του και να καταγραφούν οι πληροφορίες που περιέχονται στη μνήμη του, για να αναλυθούν. Κάτι αντίστοιχο δεν είναι δυνατό να πραγματοποιηθεί σε ένα δίκτυο, λόγω του όγκου των δεδομένων καθώς και ότι τα δεδομένα είναι δυναμικά, νέα δεδομένα παράγονται συνεχώς στο δίκτυο. Πολλές φορές οι πληροφορίες που περιέχει ο κάθε υπολογιστής του δικτύου χρησιμοποιούνται επιπρόσθετα για να συμπληρώσουν ή να επιβεβαιώσουν πληροφορίες από άλλες πηγές του δικτύου.

Σε ένα δίκτυο τα δεδομένα-πειστήρια δεν είναι συγκεντρωμένα σε μια συσκευή αλλά βρίσκονται διάσπαρτα στις διάφορες συσκευές του δικτύου (firewalls, routers,IDSs κλπ). Η ειδοποιός διαφορά στη Δικανική Δικτύων είναι ότι το δίκτυο πρέπει να παραμείνει ενεργό (live network) κατά την διάρκεια τη διερεύνησης του. Στη Δικανική Υπολογιστών ο υπολογιστής είναι επιθυμητό να απομονωθεί από

οτιδήποτε μπορεί να επηρεάσει τα δεδομένα του και επομένως το καλώδιο δικτύου θα πρέπει να αφαιρεθεί. Ωστόσο η διακοπή ενός εταιρικού δικτύου από το διαδίκτυο δεν είναι κάτι το επιθυμητό καθώς το κόστος από μια τέτοια ενέργεια είναι πολύ υψηλό. Γίνεται αντιληπτό ότι ένα δίκτυο δεν μπορεί να απομονωθεί με τον ίδιο τρόπο που ένας υπολογιστής απομονώνεται για την πραγματοποίηση της διερεύνησης. Η Δικανική Δικτύων πρέπει να πραγματοποιηθεί σε ενεργό δίκτυο και σε πραγματικό χρόνο [E1].

Η παρακολούθηση και η καταγραφή της δικτυακής κίνησης σε πραγματικό χρόνο, είναι ένα απαραίτητο κομμάτι της Δικανικής Δικτύων αλλά υπάρχουν κάποιες δυσκολίες, οι οποίες πρέπει πρώτα να ξεπεραστούν. Σε δίκτυα με μεγάλη ροή δεδομένων απαιτούνται πολύ μεγάλες αποθηκευτικές μονάδες για την πλήρη καταγραφή της κίνησης. Επίσης, σε μερικές περιπτώσεις η καταγραφή της κίνησης του δικτύου μπορεί να μην είναι νόμιμη, καθώς μπορεί να εμπεριέχονται ευαίσθητα ή προσωπικά δεδομένα. [Bru05]

Πολλές φορές η χρήση κρυπτογράφησης στα δεδομένα ενός υπολογιστή, μπορεί να δυσκολέψει ή και να αποτρέψει το έργο της ανάλυσης τους. Ωστόσο η κρυπτογράφηση είναι περισσότερο χρησιμοποιούμενη στα δεδομένα που πρόκειται να μεταφερθούν μέσω δικτύου παρά στα δεδομένα ενός μεμονωμένου υπολογιστή.

2.3 Μοντέλα και Αρχιτεκτονικές

Στον παρόν υποκεφάλαιο περιγράφονται κάποια μοντέλα, που έχουν προταθεί από διάφορους ερευνητές του χώρου. Παρόλο που δεν υπάρχει κάποια προτυποποίηση, όλα τα μοντέλα θα πρέπει να παρέχουν τρόπους συλλογής των στοιχείων από το δίκτυο, αποθήκευσης και ανάλυσης τους.

2.3.1 Το μοντέλο του Scott Redding

Ο Scott Redding προτείνει ένα μοντέλο βασισμένο σε ένα peer-to-peer (P2P) πλαίσιο (framework) για το σκοπό της παρακολούθησης του δικτύου και την εφαρμογή της δικανικής δικτύων (Network Forensics) [Red05]. Για την

αναγνώριση κακόβουλης δραστηριότητας χρησιμοποιούνται εργαλεία βασισμένα στον υπολογιστή ξενιστή (host based security tools). Όλοι οι υπολογιστές στο P2P δίκτυο μπορούν να ανταλλάσουν και να μοιράζονται τα ύποπτα συμβάντα που ανιχνεύει ο καθένας, με σκοπό την ανάλυση των συμβάντων, την αναγνώριση επιθέσεων, την κοινή γνώση χρήσιμων πληροφοριών, με στόχο την ασφάλεια του δικτύου αλλά και την διατήρηση αυτών των στοιχείων.

Ένα P2P δίκτυο χρησιμοποιεί όλους τους υπολογιστές (peers) του δικτύου για να συλλέξει στοιχεία από συμβάντα που συνέβησαν στον καθένα από αυτούς και να τα αναλύσει για το σκοπό της δικανικής δικτύων (Network Forensics). Ως συμβάν ασφαλείας θεωρείται οποιοδήποτε περιστατικό τραβήξει την προσοχή κάποιου μηχανισμού ασφαλείας στον εκάστοτε υπολογιστή. Η εφαρμογή της δικανικής δικτύων σε ένα P2P περιβάλλον, βασίζεται στην συνεργασία όσο το δυνατόν περισσότερων υπολογιστών που ανήκουν στην ίδια ομάδα. Μια ομάδα αποτελείται από ένα σύνολο υπολογιστών οι οποίοι μοιράζονται κάποιο κοινό χαρακτηριστικό, όπως, το λειτουργικό σύστημα, ομοιότητες στο υλικό που χρησιμοποιούν, το υποδίκτυο στο οποίο ανήκουν ή κάποιο άλλο χαρακτηριστικό. Κάθε υπολογιστής μπορεί να είναι μέλος σε περισσότερες από μια ομάδες στο P2P δίκτυο και να συνεισφέρει δεδομένα για τον προσδιορισμό της κατάστασης των ομάδων του δικτύου. Η απόκτηση δεδομένων πραγματοποιείται μέσω των υπαρχόντων εφαρμογών ασφαλείας που διαθέτει ο κάθε υπολογιστής και η διακίνηση τους στα μέλη των ομάδων γίνεται μέσω του P2P δικτύου. Ο κάθε υπολογιστής αποφασίζει αυτόνομα για το αν μια δραστηριότητα είναι ύποπτη ή παρουσιάζει κάποιες ανωμαλίες. Με αυτόν τον τρόπο οι υπολογιστές αποτελούν τους αισθητήρες του δικτύου και παρόλο που αυτή δεν είναι η πρωταρχική τους λειτουργία, έχουν την ικανότητα να συλλέγουν δικτυακή κίνηση, την οποία θα αναλύουν όταν ο επεξεργαστής τους θα είναι ανενεργός από άλλες λειτουργίες.

Η διαδικασία της δικανικής δικτύων, σύμφωνα με τον Scott Redding, χωρίζεται σε πέντε διακριτές φάσεις [Red05].

1. **Η ανακάλυψη ενός συμβάντος,** για το οποίο ο αμυντικός μηχανισμός ενός υπολογιστή του δικτύου εξέδωσε μια προειδοποίηση (alert). Τα στοιχειά που προέκυψαν από την προειδοποίηση καταγράφονται και κανονικοποιούνται σε μια στάνταρ XML μορφή, ώστε να μπορούν να τα

επεξεργαστούν και οι υπόλοιποι υπολογιστές της ομάδας. Η απόκτηση πληροφοριών για το συμβάν, μπορεί να χωριστεί σε μηχανισμούς δύο επιπέδων. Το πρώτο επίπεδο περιλαμβάνει τους μηχανισμούς ασφαλείας που υπάρχουν σε έναν τυπικό υπολογιστή όπως, τείχη προστασίας (host-based firewalls), **αντιικά** προγράμματα και συστήματα ανίχνευσης εισβολών (IDS - Intrusion Detection Systems). Τα συμβάντα που ανιχνεύονται από τους μηχανισμούς του πρώτου επιπέδου, θεωρούνται σημαντικά και πρέπει να αναφέρονται σε όλα τα μέλη της ομάδας. Το δεύτερο επίπεδο περιλαμβάνει μηχανισμούς που ενεργοποιούνται μετά από ένα συμβάν ή μια σειρά συμβάντων, τα οποία κρίθηκαν από τους μηχανισμούς του πρώτου επιπέδου ότι χρειάζονται περαιτέρω συγκέντρωση στοιχείων. Οι περαιτέρω πληροφορίες που απαιτούνται συλλέγονται από προγράμματα συλλογής πακέτων (packet capturing) όπως το snort, το tcpdump και το snoop.

2. **Μετάδοση του συμβάντος στα υπόλοιπα μέλη.** Το P2P δίκτυο είναι έτσι σχεδιασμένο, ώστε η κανονικοποιημένη XML έκδοση των στοιχείων του συμβάντος, να μεταδοθεί στα υπόλοιπα μέλη. Αυτό γίνεται χωρίς καμία προεργασία σχετικά με την ταυτότητα ή την θέση των άλλων μελών. Η διακίνηση των πληροφοριών σε ένα P2P δίκτυο πραγματοποιείται χωρίς την ύπαρξη κάποιου κεντρικού συστήματος διαχείρισης και συντονισμού, σε αντίθεση με ότι συμβαίνει στα δίκτυα που βασίζονται στην client-server αρχιτεκτονική. Με αυτό τον τρόπο είναι δυνατή η ανακάλυψη νέων μελών και η δυνατότητα άμεσης επικοινωνίας μεταξύ τους, χωρίς την ανάγκη κάποιου ενδιάμεσου.

3. **Αποθήκευση των δεδομένων.** Οι πληροφορίες που σχετίζονται με ένα συμβάν, θα πρέπει να αρχειοθετούνται με τέτοιο τρόπο, ώστε να μπορεί να διεξαχθεί έρευνα χωρίς να υπάρχει αμφιβολία για την ακεραιότητα των στοιχείων. Δημιουργώντας βάσεις δεδομένων σε κάθε υπολογιστή, οι οποίες θα περιλαμβάνουν στοιχεία για όλες τις ομάδες στις οποίες ανήκει ο κάθε υπολογιστής, μπορούν να επιβεβαιώσουν την ακεραιότητα των δεδομένων. Η αρχειοθέτηση των πληροφοριών θα πρέπει να περιλαμβάνει δυο ειδών εγγραφές: τις εγγραφές επιθεώρησης (audit records), οι οποίες

χρησιμοποιούνται για την αναδημιουργία ενός συμβάντος και απαιτούν πιο ακριβείς πληροφορίες, και οι αναλυτικές εγγραφές. Αντίγραφα δηλαδή πληροφοριών ενός συμβάντος που έστειλε ένα μέλος και τα οποία χρησιμεύουν στην εξακρίβωση, αν κακόβουλη δραστηριότητα βρίσκεται σε εξέλιξη. Η αξία των αναλυτικών εγγραφών μειώνεται καθώς περνάει ο χρόνος και μπορούν να συνοψιστούν ή και να διαγραφούν.

4. **Η ανάλυση των δεδομένων.** Καθώς ένας υπολογιστής λάβει πληροφορίες για ένα συμβάν από κάποιο άλλο μέλος, προσπαθεί να εξετάσει και να συσχετίσει το συμβάν με άλλα που είναι αρχειοθετημένα στη βάση δεδομένων του, ώστε να διαπιστωθεί αν αξίζει να εξεταστεί με μεγαλύτερη λεπτομέρεια. Η διαδικασία της ανάλυσης προσδιορίζει αν ένα συμβάν είναι υψηλής προτεραιότητας και η διαδικασία της ανάλυσης ξεκινάει κάθε φορά που φτάνει μια αναφορά ενός συμβάντος από το P2P δίκτυο. Για να προσδιοριστεί αν ένα συμβάν είναι υψηλής προτεραιότητας, χρησιμοποιούνται δυο τεχνικές ανάλυσης: η στατιστική ανάλυση και η ανάλυση που βασίζεται σε κανόνες (rule-based). Η στατιστική ανάλυση, χρησιμοποιώντας ως μέτρο σύγκρισης αυτό που στατιστικά έχει τεθεί ως φυσιολογική χρήση του συστήματος, προσπαθεί να προσδιορίσει αν ένα συμβάν είναι υψηλής προτεραιότητας. Η τεχνική αυτή υποθέτει ότι η οποιαδήποτε προσπάθεια εκμετάλλευσης των αδυναμιών του συστήματος, θα περιλαμβάνει ασυνήθιστες ενέργειες ή θα παραβιάζει τις πολιτικές ασφαλείας του συστήματος, καθιστώντας το συμβάν ύποπτο. Η τεχνική ανάλυσης που βασίζεται σε κανόνες (rule-based), χρησιμοποιεί τις υπάρχουσες γνώσεις για προηγούμενα γνωστές μεθοδολογίες επιθέσεων. Αν ένα συμβάν θεωρηθεί ότι ακολουθεί ένα συγκεκριμένο σενάριο επίθεσης τότε αυτόματα σημειώνεται ως συμβάν υψηλής προτεραιότητας. Όταν από την ανάλυση ενός συμβάντος προκύψει ότι πρόκειται για περιστατικό υψηλής προτεραιότητας, ο υπολογιστής-μέλος που πραγματοποίησε την ανάλυση, αποστέλλει μια προειδοποίηση σε όλα τα μέλη των ομάδων που συμμετέχει, για την περαιτέρω συλλογή πληροφοριών σχετικών με το συμβάν.

5. **Αναφορά των συμπερασμάτων.** Κάθε μέλος αναφέρει στα υπόλοιπα μέλη τα συμπεράσματα που προέκυψαν από την ανάλυση, ώστε να δημιουργηθεί μια πλήρης εικόνα για όλη την ομάδα.

2.3.2 Το μοντέλο των Ren-Jin

Οι Wei Ren και Hai Jin, δημιούργησαν ένα μοντέλο Δικανικής Δικτύων που βασίζεται σε ένα Honeynet σύστημα. Ένα σύστημα Honeynet λειτουργεί ως δόλωμα προσελκύοντας επίδοξους εισβολείς, προσπαθώντας να αποκτήσει πληροφορίες σχετικά με νέους τύπους επιθέσεων. Ένα σύστημα Δικανικής Δικτύων μπορεί να αναλύσει και να αναδημιουργήσει την επίθεση του εισβολέα. Τα δυο αυτά συστήματα συνδυασμένα μεταξύ τους μπορούν να δημιουργήσουν ένα ενεργό σύστημα με δυνατότητα να μαθαίνει, το οποίο θα σχεδιάζει το προφίλ και τα χαρακτηριστικά των επιθέσεων και θα διεξάγει έρευνα για τον προσδιορισμό της προέλευσης της επίθεσης [Ren05].

Η προσέγγιση που ακολουθείται σε αυτό το μοντέλο, είναι η αποτελεσματική καταγραφή της κίνησης του δικτύου, η οποία θα συλλέγεται από διάφορους υπολογιστές-κατασκόπους (agents) κατανεμημένους στο δίκτυο. Στη συνέχεια θα πραγματοποιείται ανάλυση της καταγεγραμμένης κίνησης προσαρμοσμένη στις ανάγκες του χρήστη. Τέσσερα βασικά στοιχεία συνθέτουν το μοντέλο αυτό: ο network forensics server, οι network forensics agents, ο network forensics monitor και ο network forensics investigator [Ren05].

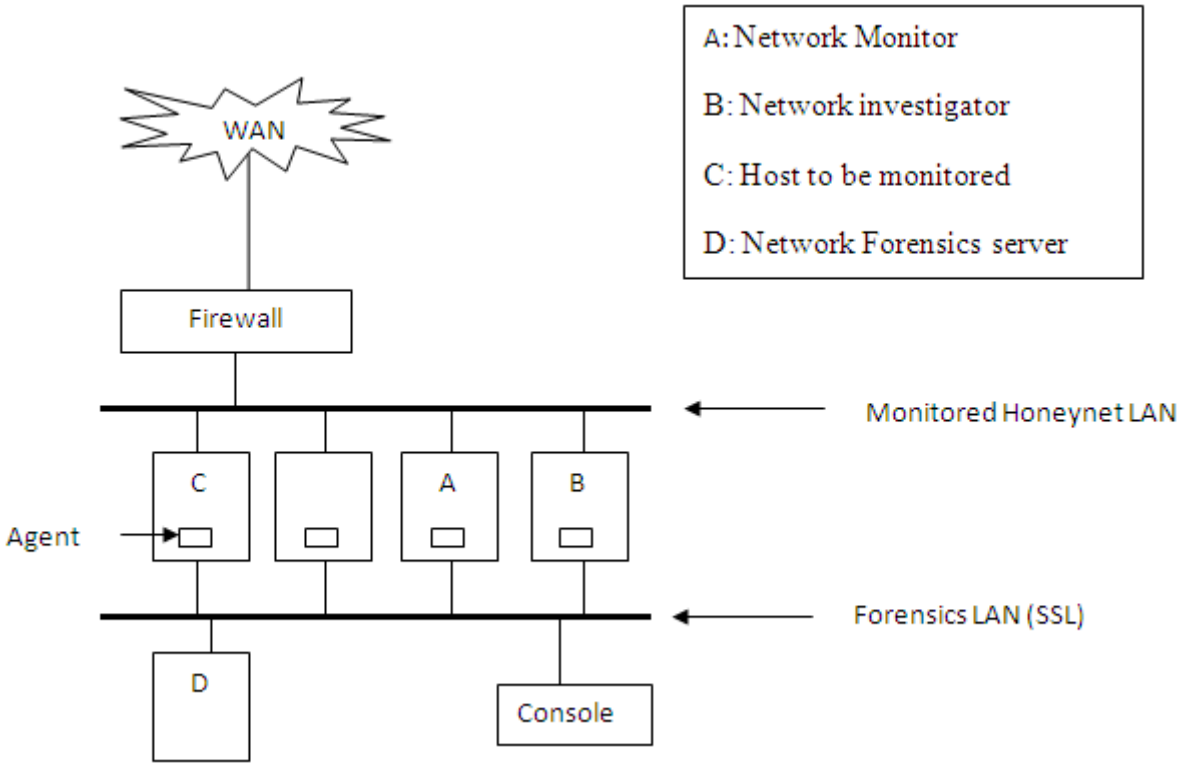
Ο **network forensics server** περιέχει τα δεδομένα και είναι υπεύθυνος για την ανάλυση τους. Καθοδηγεί τον packet filter του δικτύου και συλλέγει τη συμπεριφορά από το network monitor. Επίσης μπορεί να πυροδοτήσει το πρόγραμμα διερεύνησης στον network investigator, στην περίπτωση επίθεσης.

Οι **network forensics agents** είναι υπεύθυνοι για τη συλλογή των δεδομένων, την εξαγωγή των δεδομένων και την ασφαλή μεταφορά τους στο server. Οι agents τοποθετούνται στον υπολογιστή που παρακολουθείται και στο δίκτυο.

Ο **network forensics monitor** είναι το σύστημα που συλλέγει πακέτα, συλλέγοντας προσαρμοστικά την κίνηση του δικτύου.

Ο **network forensics investigator** είναι η συσκευή η οποία διεξάγει έρευνα στο δίκτυο, σε ένα συγκεκριμένο στόχο όταν ο server δώσει την εντολή. Επίσης διεξάγει έρευνα σε πραγματικό χρόνο ως αντίδραση σε πιθανή εισβολή στο δίκτυο.

Στην εικόνα φαίνεται η αρχιτεκτονική του συστήματος, με δυο τοπικά δίκτυα. Το πρώτο δίκτυο είναι το Honeynet το οποίο παρακολουθείται και το άλλο το Forensics LAN το οποίο είναι υψηλής ταχύτητας και χρησιμοποιεί SSL (Secure Socket Layer) για ασφαλή μεταφορά των δεδομένων.



Εικόνα 2.1. Αρχιτεκτονική Συστήματος

Το σύστημα Δικανικής Δικτύων ενσωματώνει τα αρχεία καταγραφής από το Honeynet όπως, server logs, host logs και ειδοποιήσεις από το IDS, σε μια βάση δεδομένων. Διάφορες τεχνικές εξόρυξης δεδομένων μπορούν να χρησιμοποιηθούν για βρεθούν πληροφορίες σχετικές με τον επιτιθέμενο όπως, IP διεύθυνση, MAC διεύθυνση και οι θύρες που χρησιμοποιήθηκαν για την επίθεση.

Η μονάδα που ευθύνεται για τη συλλογή των δεδομένων έχει τη δυνατότητα να καταγράφει πλήρως τη δικτυακή κίνηση, το οποίο απαιτεί μεγάλο αποθηκευτικό

χώρο. Ωστόσο υπάρχει η δυνατότητα να αποθηκεύονται επιλεκτικά κάποια δεδομένα, όπως οι διευθύνσεις προέλευσης-προορισμού, θύρες που χρησιμοποιήθηκαν, η διάρκεια και τα bytes που μεταφέρθηκαν για κάθε TCP σύνδεση. Επίσης εφαρμόζοντας κατάλληλα φίλτρα μπορούμε να αποφθεχθούν πακέτα που δεν παρουσιάζουν ενδιαφέρον.

Ειδικά εργαλεία μπορούν να οργανώσουν τα πακέτα σε ξεχωριστές συνδέσεις (επιπέδου μεταφοράς) μεταξύ των μηχανών. Η κυριότερη δουλειά της ανάλυσης είναι το λεγόμενο protocol parsing. Στα πρωτόκολλα POP3, HTTP, FTP και TELNET πρέπει να δοθεί ιδιαίτερη προσοχή κατά διαδικασία της ανάλυσης. Μετά το protocol parsing είναι πιθανό να βρεθεί κάποιο κρυφό κανάλι (covert channel) ή δεδομένα που κρύβονται στην κίνηση του δικτύου. Κατά την διεξαγωγή της έρευνας είναι δυνατόν με τη χρήση κάποιων μεθόδων, να ακολουθηθούν τα ίχνη μιας σταθερής ροής από ανώνυμα πακέτα πίσω στην πηγή τους. Η εύρεση της προέλευσης των IP διευθύνσεων (IP trace back) και η χαρτογράφηση των IP διευθύνσεων σε μια γεωγραφική τοποθεσία είναι από τα πιο σημαντικά στοιχεία του network forensics investigator. Μόλις το IDS στείλει μια προειδοποίηση, ο network forensics server στέλνει την εντολή στον network forensics investigator για τη διεξαγωγή έρευνας σε πραγματικό χρόνο.

2.3.3 Το μοντέλο του Ren Wei

Ο Ren Wei παρουσιάζει ένα εννοιολογικό μοντέλο για την ανάπτυξη ενός συστήματος Δικανικής Δικτύων, το οποίο μπορεί να παρέχει καθοδήγηση για την υλοποίηση και την τυποποίηση της διαδικασίας της Δικανικής Δικτύων. Ένα σύστημα Δικανικής Δικτύων θα πρέπει να μπορεί να πραγματοποιεί τρείς βασικές εργασίες: να συλλέγει την κίνηση του δικτύου, να αναλύει την κίνηση σύμφωνα με τις ανάγκες του χρήστη και να επιτρέπει στο χρήστη του συστήματος να ανακαλύπτει χρήσιμες πληροφορίες σχετικά με την κίνηση που αναλύθηκε [Ren04].

Από την άποψη των λειτουργιών ενός συστήματος Δικανικής Δικτύων, αυτό θα πρέπει να μπορεί να πραγματοποιεί:

1. **Διερεύνηση του δικτύου.** Πριν ακόμα συγκεντρωθούν αρκετά στοιχεία, κάποια διερεύνηση θα πρέπει να πραγματοποιείται με τη χρήση εργαλείων αναζήτησης (browser tools, ftp tools, email tools), τα οποία μπορεί να είναι ενσωματωμένα στο σύστημα.

2. **Τοπογράφηση του δικτύου.** Για την τοπογράφηση του δικτύου χρησιμοποιούνται εργαλεία ανεύρεσης αποτυπωμάτων (footprinting tools), όπως τα whois, nslookup, traceroute. Στη συνέχεια εργαλεία σάρωσης (scanning tools), όπως τα nmap, Hping2, χρειάζεται να περιλαμβάνονται στο συνολικό πακέτο εργαλείων συστήματος Δικανικής Δικτύων. Τέλος ειδικά εργαλεία απαρίθμησης (enumeration tools) θα πρέπει να περιλαμβάνονται, για την απαρίθμηση του NetBIOS και του SNMP πρωτοκόλλου.

3. **Καταγραφή της δικτυακής κίνησης.** Η κίνηση του δικτύου θα πρέπει να καταγράφεται πλήρως από το σύστημα, έχοντας παράλληλα τη δυνατότητα να φιλτράρει την κίνηση με βάση κάποιους κανόνες.

4. **Συσσωμάτωση των δεδομένων.** Η καταγραφή δεδομένων από διαφορετικές τοποθεσίες του δικτύου παρέχουν διαφορετικές πληροφορίες σχετικά με το προφίλ του επιτιθέμενου. Η ανάλυση του συνόλου των δεδομένων που προέρχονται από διαφορετικές πηγές (όπως firewalls, IDSs, packet sniffers) μπορούν να δημιουργήσουν μια αλληλουχία στοιχείων και να παρουσιάσουν όλα τα βήματα της επίθεσης. Το σύστημα Δικανικής Δικτύων θα πρέπει να αποθηκεύει τα συσσωματωμένα δεδομένα ομοιόμορφα σε μια βάση δεδομένων.

5. **Πρόβλεψη μελλοντικών επιθέσεων.** Ο κάθε επιτιθέμενος ή η κάθε ομάδα επιτιθέμενων, έχει πάντα κάποια χαρακτηριστικά, όπως τα εργαλεία που χρησιμοποίησε για την επίθεση, συχνότερα χρησιμοποιημένες τεχνικές ή κάποια χαρακτηριστικά ίχνη που άφησε κατά την διάρκεια της επίθεσης. Με βάση αυτά τα στοιχεία το σύστημα θα πρέπει να παρέχει μια πρόβλεψη για μελλοντικές επιθέσεις.

6. **Ανακάλυψη ανώμαλων προτύπων.** Τα καταγεγραμμένα δεδομένα μπορούν να εξεταστούν με διάφορες τεχνικές εξόρυξης δεδομένων για ανώμαλα πρότυπα (anomaly patterns), τα οποία θα επηρεάσουν το σύνολο των κανόνων του firewall και του IDS.

Από την άποψη της αρχιτεκτονικής του συστήματος, ο forensics server, ο οποίος θα είναι παρατεταγμένος σε ένα κατανεμημένο δίκτυο, θα αποθηκεύει τα δεδομένα που θα προέρχονται από τους υπολογιστές-πράκτορες (forensics agents). Η σημαντικότερη λειτουργία του server είναι να ανιχνεύει την πηγή της κακόβουλης δραστηριότητας. Οι πράκτορες θα είναι τοποθετημένοι σε σημεία κλειδιά του δικτύου και θα συλλέγουν τη δικτυακή κίνηση η οποία θα αποστέλλεται στο server.

2.3.4 Το μοντέλο των Ahmad Almulhem και Issa Traore

Το μοντέλο αυτό, μπορεί να εφαρμοστεί σε ένα τυπικό δίκτυο με ένα πλήθος υπολογιστών και περιλαμβάνει τρία βασικά μέρη που το απαρτίζουν:

1. **Marking module.** Αυτή η μονάδα είναι το σημείο εισόδου του δικτύου. Καθώς τα πακέτα εισέρχονται στο δίκτυο, αυτά εξετάζονται από τη μονάδα μαρκαρίσματος και χαρακτηρίζονται ως φιλικά ή κακόβουλα. Η μονάδα βασίζεται σε ένα σύνολο αισθητήρων , οι οποίοι διατηρούν μια λίστα με ύποπτες IP διευθύνσεις. Αν η IP διεύθυνση του πακέτου περιέχεται στην λίστα, τότε το πακέτο μαρκάρεται ως κακόβουλο τροποποιώντας το πεδίο TOS (Type of Service) στην IP κεφαλίδα. Η λίστα με τις IP διευθύνσεις, είναι μια δομή δεδομένων, η οποία διατηρεί τις διευθύνσεις που έχουν αναφερθεί ως ύποπτες από τουλάχιστον ένα αισθητήρα. Η λίστα κρατάει για κάθε IP διεύθυνση το βαθμό προτεραιότητας (υψηλή, μέτρια, χαμηλή), έναν αριθμό που δείχνει πόσες φορές έχει αναφερθεί η συγκεκριμένη IP και ένα χρονόμετρο, το οποίο όταν φτάσει στο μηδέν αφαιρείται η διεύθυνση IP από τη λίστα.

2. **Capture module.** Η μονάδα συλλογής πακέτων βρίσκεται σε κάθε υπολογιστή και μόλις εντοπιστεί ένα μαρκαρισμένο πακέτο, το στέλνει στη

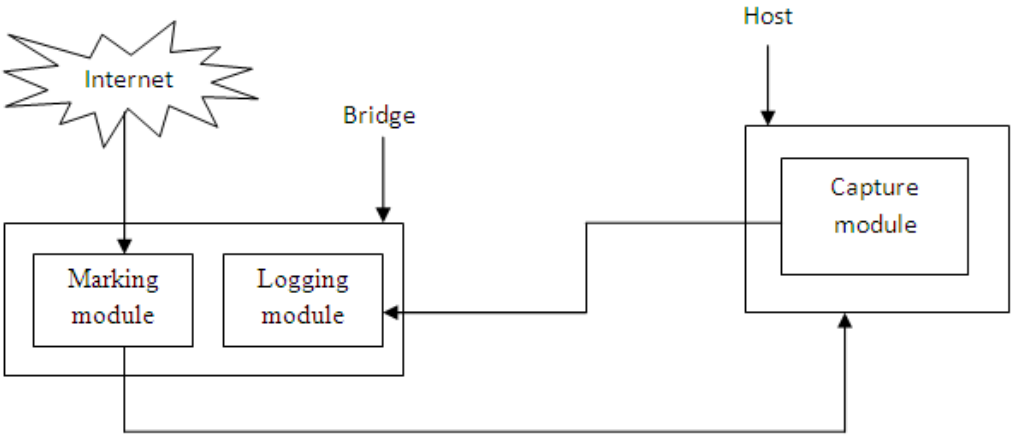
μονάδα καταχώρησης για την ασφαλή φύλαξη του. Η ύπαρξη μονάδας συλλογής πακέτων σε κάθε υπολογιστή, δίνει λύση στο πρόβλημα της χρήσης κρυπτογραφημένων καναλιών από τους επιτιθέμενους, για να κρύψουν τις δραστηριότητες τους, καθώς μόνο στον εκάστοτε υπολογιστή μπορεί να αναστραφεί η κρυπτογράφηση και να καταγραφούν πλήρως οι ενέργειες του επιτιθέμενου.

3. **Logging module.** Αυτή η μονάδα αποτελεί τον αποθηκευτικό χώρο του συστήματος, όπου τοποθετούνται τα δεδομένα από τις επιθέσεις που καταγράφονται. Στην ιδανική περίπτωση θα πρέπει να παρέχει αξιόπιστες πληροφορίες για κάθε πραγματοποιημένη επίθεση. Εσωτερικά η μονάδα θα χωρίζεται σε τρείς ξεχωριστούς καταχωρητές:

   (1) Host Logger: Αυτός ο καταχωρητής είναι υπεύθυνος για τη φύλαξη των δεδομένων που προέρχονται από τα Capture modules. Θα περιέχει αναλυτικές πληροφορίες που θα σχετίζονται με πραγματικά περιστατικά επιθέσεων και επομένως οι απαιτήσεις σε αποθηκευτικό χώρο είναι μικρές.

   (2) Sensor Logger: Σε αυτό το τμήμα θα καταχωρούνται προειδοποιήσεις (alerts) από τους αισθητήρες του δικτύου. Μια τυπική προειδοποίηση είναι ένα μήνυμα μιας γραμμής, που παρέχει μια γρήγορη διάγνωση της επίθεσης.

   (3) Raw Logger: Αυτός ο καταχωρητής αποτελεί την έσχατη λύση, όταν οι υπόλοιποι καταχωρητές αποτύχουν. Αποθηκεύει πακέτα κατευθείαν όπως αυτά εισέρχονται στο δίκτυο και απαιτεί πολύ μεγάλο αποθηκευτικό χώρο. [Ahm05]



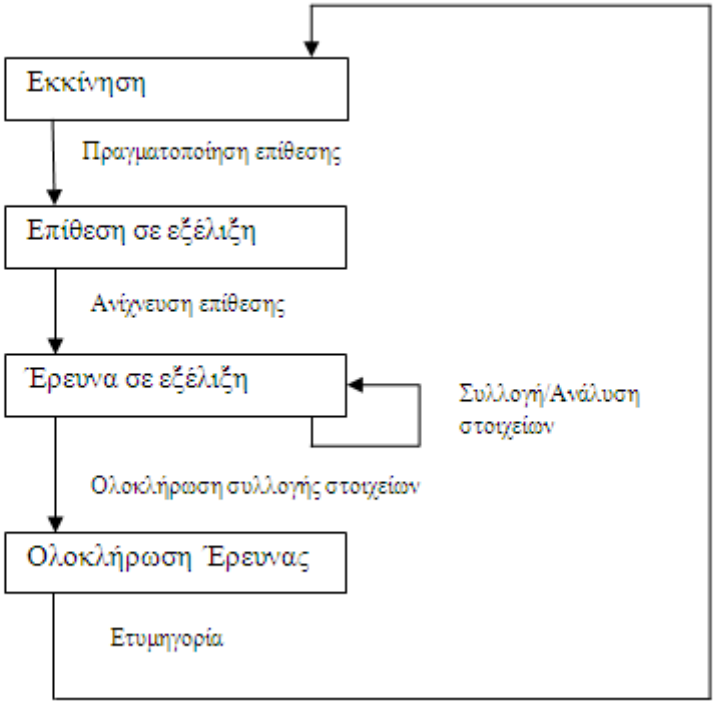
Εικόνα 2.2. Αρχιτεκτονική του συστήματος

2.3.5 Μοντελοποίηση της Δικανικής Δικτύων και Υπολογιστών χρησιμοποιώντας Honeytraps

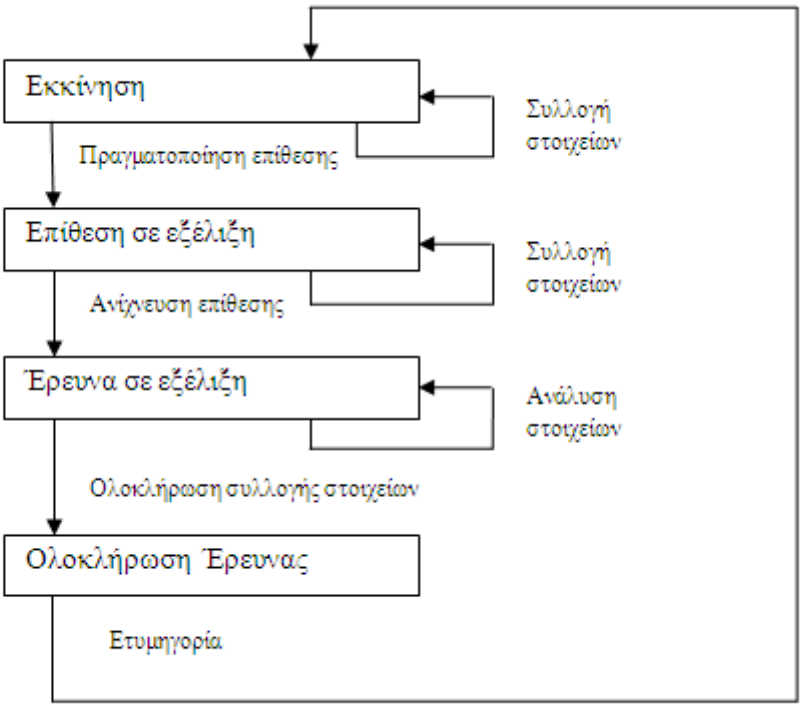
Παραδοσιακά, οι προσπάθειες για μεγαλύτερη ασφάλεια σε ένα σύστημα, επικεντρώνονταν στις ενέργειες που λαμβάνονταν πριν πραγματοποιηθεί μια επίθεση, ώστε να προστατεύσουν τους πόρους και τις πληροφορίες, από κακόβουλη πρόσβαση ή χρήση. Πλέον, οι προσπάθειες επικεντρώνονται στην αναγνώριση των επιθέσεων και στις τεχνολογίες απόκρισης κατά τη διάρκεια των επιθέσεων, ώστε να προστατεύσουν τους πόρους και τις πληροφορίες του συστήματος [Jou00, Vig99]. Από την άλλη μεριά, η Δικανική Δικτύων και Υπολογιστών (CNF – Computer and Network Forensics), επικεντρώνεται στη συλλογή πληροφοριών, σχετικών με μια επίθεση ή εισβολή, παρά στο να παράσχει άμεση προστασία στους πόρους και τις πληροφορίες του συστήματος. Οι προσπάθειες δηλαδή, εστιάζουν στις ενέργειες που θα γίνουν μετά την κακόβουλη δραστηριότητα, παρά στις δραστηριότητες που συμβαίνουν πριν ή κατά τη διάρκεια της επίθεσης.

Οι Manzano και Yasinsac, πρότειναν κάποιες πολιτικές και τεχνικές, οι οποίες εφαρμόζονται πριν, κατά τη διάρκεια και μετά την πραγματοποίηση κακόβουλης

δραστηριότητας, επεκτείνοντας το πεδίο δράσης του κλασικού μοντέλου CNF [Man01].



Εικόνα 2.3. Παραδοσιακό Μοντέλο



Εικόνα 2.4. Νέο Μοντέλο

Στο παραδοσιακό μοντέλο (εικόνα 2.3), η συλλογή στοιχείων ξεκινούσε μετά την επίθεση ή όταν γινόταν η αναγνώριση της. Στο νέο μοντέλο (εικόνα 2.4), η δραστηριότητα της συλλογής στοιχείων ξεκινάει πριν συμβεί η επίθεση, έτσι η κύρια δραστηριότητα που πραγματοποιείται μετά την επίθεση είναι η ανάλυση των στοιχείων που έχουν ήδη συλλεχθεί, επιτρέποντας παράλληλα στην όλη διαδικασία να είναι συνεχής. Οι Alec Yasinsac και Yanet Manzano, χρησιμοποιώντας αυτό το μοντέλο, προτείνουν δυο αρχιτεκτονικές, οι οποίες επιτρέπουν τη χρήση των Honeytraps ως ένα εργαλείο στη Δικανική Δικτύων [Man02]. Εδώ κρίνεται σκόπιμο να γίνει μια σύντομη αναφορά των Honeytraps, Honeypots και Honeynets, γνωστές τεχνολογίες εξαπάτησης.

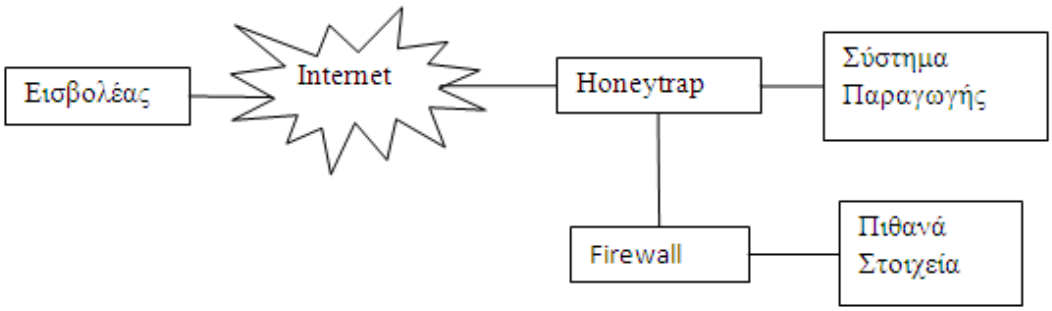
Τα Honeytraps, είναι συστήματα, τα οποία έχουν σχεδιαστεί για να προσελκύουν επίδοξους εισβολείς και να δέχονται επιθέσεις, χωρίς να θέτουν σε κίνδυνο το πραγματικό σύστημα. Παράλληλα, δίνουν τη δυνατότητα να συλλέγονται πληροφορίες, σχετικά με τις δραστηριότητες και τις τεχνικές που χρησιμοποιούν οι εισβολείς και οι ομάδες στις οποίες ανήκουν. Ο όρος Honeytraps είναι γενικός και αναφέρετε στα Honeypots και Honeynets. Τα Honeypots, είναι συστήματα προσωπικών υπολογιστών (hosts) που προσελκύουν, κατά κάποιο τρόπο τους επιτιθέμενους, προσομοιώνοντας κάποια γνωστή αδυναμία στο σύστημα τους. Τα συστήματα αυτά είναι τροποποιημένα έτσι ώστε οι ενέργειες του εισβολέα να παρακολουθούνται και να καταγράφονται με ασφάλεια. Δεν περιέχουν πραγματικά δεδομένα ή πολύτιμα δεδομένα. Από την άλλη, τα Honeynets, είναι δίκτυα διασυνδεδεμένων Honeypot κόμβων και κόμβων παραγωγής. Οι κόμβοι παραγωγής, είναι τα πραγματικά συστήματα τα οποία προστατεύονται, καθώς τα Honeypots αποσπούν την προσοχή των επιτιθέμενων από τον πραγματικό στόχο. Τα Honeynets έχουν τον ίδιο ρόλο με τα Honeypots, συλλέγουν δηλαδή πληροφορίες για τους εισβολείς. Γενικά στα Honeytraps, πάντα εγκυμονεί ο κίνδυνος, το ίδιο το σύστημα Honeytrap, να δεχτεί επίθεση και να επέλθει στην κυριότητα του εισβολέα.

2.3.5.1 Honeytrap σε Σειριακή Αρχιτεκτονική

Στη σειριακή αρχιτεκτονική, το σύστημα Honeytrap, τοποθετείται ανάμεσα στο διαδίκτυο και στο σύστημα παραγωγής. Σε αυτή τη διάταξη, το σύστημα Honeytrap

λειτουργεί ως τείχος προστασίας. Όλοι οι αναγνωρισμένοι χρήστες φιλτράρονται στο σύστημα παραγωγής ενώ οι εισβολείς συγκρατούνται στο Honeytrap και οι δραστηριότητες τους παρακολουθούνται στο σύστημα Honeytrap και όλες οι πληροφορίες που θα συλλέγονται, θα αποστέλλονται σε ένα άλλο σύστημα, το οποίο θα προστατεύεται από firewall για να εξασφαλίζεται η ακεραιότητα των δεδομένων. Στη σειριακή αρχιτεκτονική, ο εισβολέας αναγκάζεται να περάσει μέσα από το σύστημα Honeytrap, προκειμένου να επιτεθεί στο πραγματικό σύστημα, αποκαλύπτοντας έτσι τις τεχνικές του, οι οποίες καταγράφονται.

Ένα σημαντικό χαρακτηριστικό των Honeytraps, είναι ότι δεν έχουν να κάνουν με πραγματικούς χρήστες και έτσι είναι ευκολότερη η παρακολούθηση τους. Ωστόσο, στη σειριακή αρχιτεκτονική, το Honeytrap πρέπει να χειρίζεται όλη τη κίνηση που εισέρχεται στο σύστημα παραγωγής και να επαναδρομολογεί τους εξουσιοδοτημένους χρήστες στο σύστημα παραγωγής. Για να επιτευχθεί αυτό χρειάζεται περισσότερους πόρους. Αυτή η αρχιτεκτονική, ενέχει το ρίσκο οι εισβολείς να καταφέρουν να επιτεθούν με επιτυχία στο σύστημα παραγωγής, παρά την προσπάθεια περιορισμού τους στα όρια του Honeytrap.

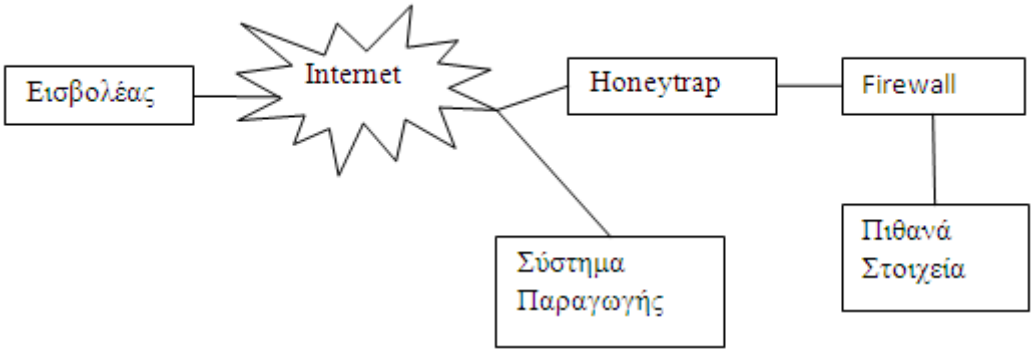


Εικόνα 2.5. Honeytrap σε Σειριακή Αρχιτεκτονική

2.3.5.2 Honeytrap σε Παράλληλη Αρχιτεκτονική

Η παράλληλη διάταξη επιτρέπει στο Honeytrap να είναι ανεξάρτητο από το σύστημα παραγωγής. Όπως και στη σειριακή αρχιτεκτονική , οι πληροφορίες που

συλλέγονται στο Honeytrap για τους εισβολείς, αποστέλλονται σε ένα ξεχωριστό προστατευόμενο σύστημα. Αυτή η αρχιτεκτονική απαιτεί λιγότερους πόρους, καθώς η κίνηση του συστήματος παραγωγής δεν περνάει μέσα από το Honeytrap. Ωστόσο, και η παράλληλη αρχιτεκτονική έχει κάποια μειονεκτήματα. Καταρχήν, για να έχει αξία και χρησιμότητα το Honeytrap στη δικανική διαδικασία, θα πρέπει και τα δύο συστήματα (Honeytrap και σύστημα παραγωγής) να δεχθούν επίθεση ξεχωριστά. Στην παράλληλη αρχιτεκτονική είναι δυσκολότερο να συσχετιστεί μια επίθεση στο Honeytrap, με μια επίθεση στο σύστημα παραγωγής, καθώς δεν υπάρχει άμεση σύνδεση μεταξύ τους όπως υπάρχει στη σειριακή αρχιτεκτονική.



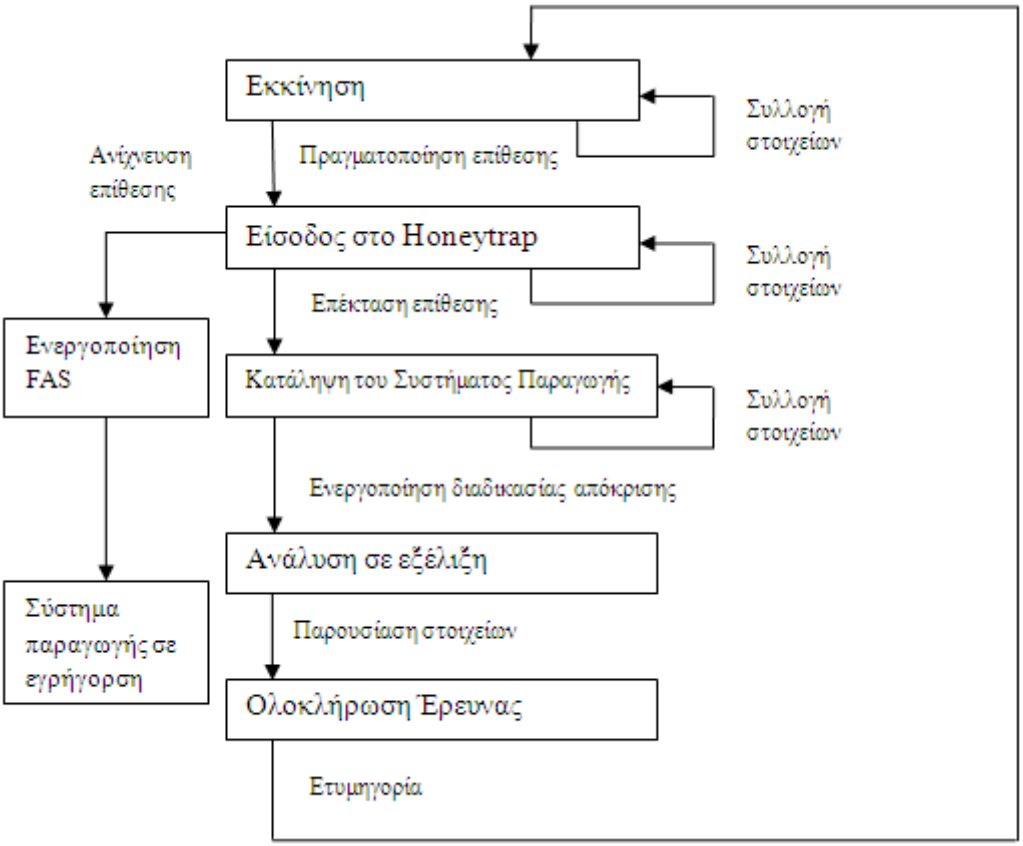
Εικόνα 2.6. Honeytrap σε Παράλληλη Αρχιτεκτονική

2.3.5.3 Δικανικά μοντέλα για σειριακή και παράλληλη αρχιτεκτονική με Honeytrap

Η χρήση των Honeytraps ως δικανικά εργαλεία και η πρόταση νέων αρχιτεκτονικών για την διευκόλυνση της δικανικής διαδικασίας, απαιτούν κάποιες προσαρμογές του μοντέλου της δικανικής διαδικασίας για την σειριακή και την παράλληλη δικανική αρχιτεκτονική με Honeytrap.

Στο σειριακό δικανικό μοντέλο, που φαίνεται στην εικόνα 2.7, η δικανική διαδικασία ξεκινά όταν ο εισβολέας εισέλθει στο Honeytrap. Μόλις ο εισβολέας αποκτήσει πρόσβαση στο Honeytrap παράγεται μια ειδοποίηση από το FAS (Forensic Alert System). Το FAS είναι ένα ενσωματωμένο σύστημα στο Honeytrap και η κύρια

λειτουργία του είναι να προειδοποιεί το σύστημα παραγωγής όταν κάποια επίθεση βρίσκεται σε εξέλιξη, ώστε να ξεκινήσει η διαδικασία παρακολούθησης και καταγραφής των δραστηριοτήτων του εισβολέα. Το σύστημα παραγωγής θα βρίσκεται σε εγρήγορση από τη στιγμή που θα λάβει την προειδοποίηση από το FAS ώστε να είναι προετοιμασμένο στην περίπτωση που επεκταθεί η επίθεση προς αυτό. Αν τελικά η επίθεση επεκταθεί στο σύστημα παραγωγής, τότε ενεργοποιείται η διαδικασία απόκρισης για να αντιμετωπίσει την επίθεση [Man01]. Αφού αντιμετωπιστεί η όλη κατάσταση, ξεκινά η διερεύνηση. Όταν συγκεντρωθούν αρκετά στοιχεία από το Honeytrap και το σύστημα παραγωγής, πραγματοποιείται ανάλυση των στοιχείων και παράγεται η αναφορά.



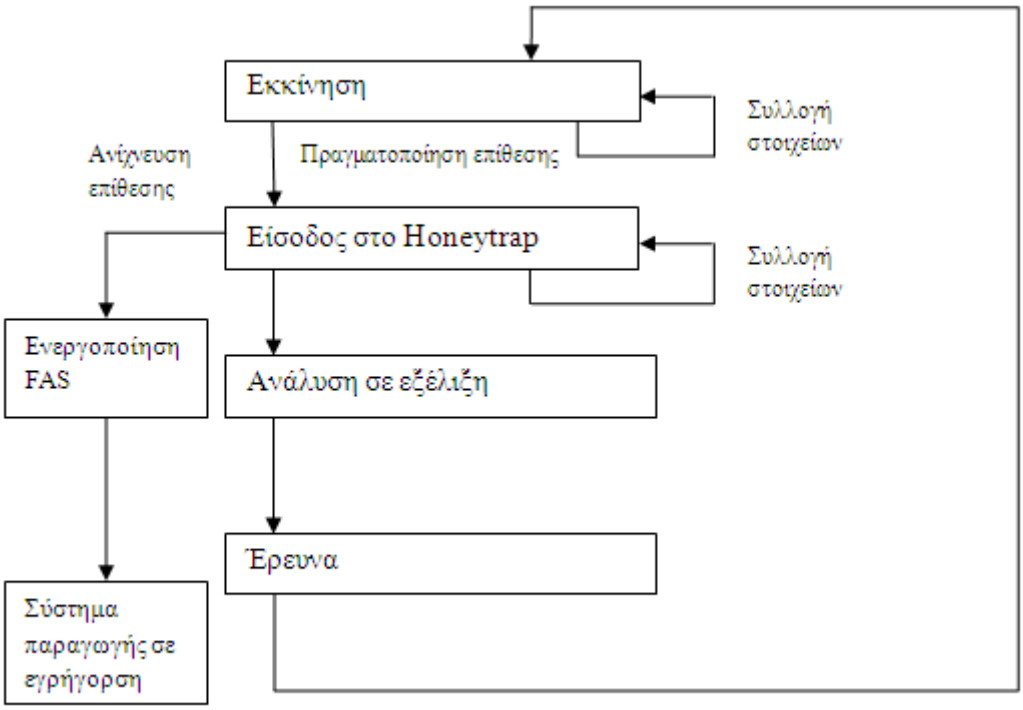
Εικόνα 2.7. Σειριακό Δικανικό Μοντέλο

Το παράλληλο δικανικό μοντέλο, είναι παρόμοιο με το σειριακό αλλά έχει μια σημαντική διαφορά. Στο παράλληλο δικανικό μοντέλο υπάρχουν δύο διεργασίες σε ταυτόχρονη εξέλιξη. Η πρώτη διεργασία (εικόνα 2.8.Α) είναι η δικανική διαδικασία του Honeytrap (HTFP – Honeytrap Forensic Process) και η δεύτερη

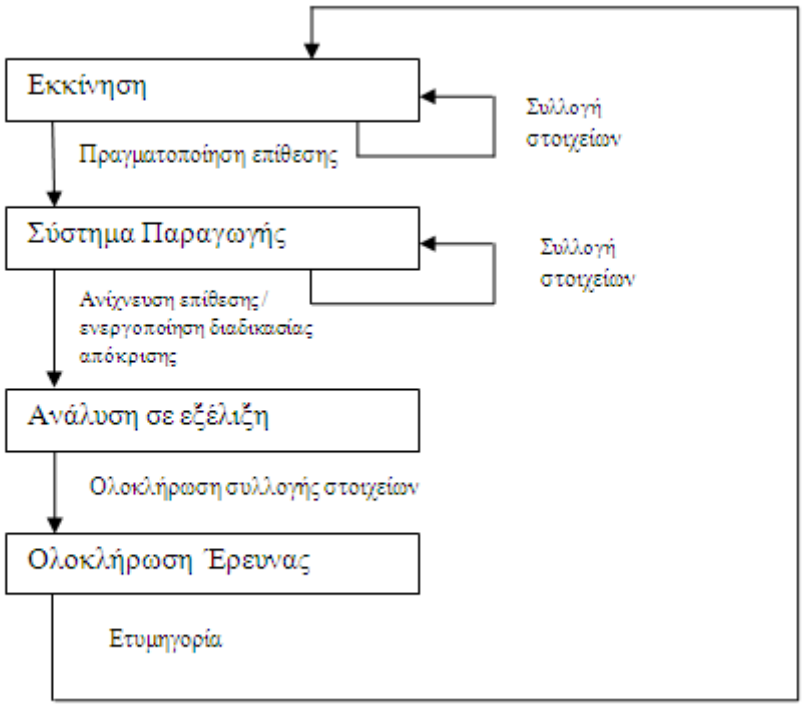
(εικόνα 2.8.B), αυτή του συστήματος παραγωγής (PSFP – Production System Forensic Process).

Η διαδικασία HTFP, ξεκινά μόλις ο εισβολέας εισέλθει στο Honeytrap και το FAS (Forensic Alert System) ενεργοποιείται. Μια προειδοποίηση παράγεται και αποστέλλεται στο σύστημα παραγωγής, ώστε να αρχίσουν να παρακολουθούνται και να καταγράφονται οι δραστηριότητες του εισβολέα. Μόλις ανιχνευθούν οι δραστηριότητες του εισβολέα, πραγματοποιείται δικανική διερεύνηση με τα στοιχεία που συλλέχθηκαν και τα αποτελέσματα αποθηκεύονται με ασφάλεια.

Η διαδικασία PSFP, ξεκινά αφού το σύστημα παραγωγής έχει παραβιαστεί και έχει ανιχνευθεί η επίθεση. Αν το Honeytrap δεχτεί πρώτο την επίθεση, τότε το σύστημα παραγωγής θα βρίσκεται ήδη σε εγρήγορση (Forensic Alert), κάνοντας ευκολότερη την ανίχνευση της επίθεσης. Μόλις η διαδικασία αντιμετώπισης της εισβολής ενεργοποιηθεί και η κατάσταση περιοριστεί, πραγματοποιείται η ανάλυση των δεδομένων που συλλέχθηκαν στο σύστημα παραγωγής και στο Honeytrap. Τέλος, παράγεται πλήρης αναφορά της ανάλυσης, με όλα τα στοιχεία και τα συμπεράσματα για τον εισβολέα.



Εικόνα 2.8.A. Παράλληλο Δικανικό Μοντέλο – Διαδικασία HTFP



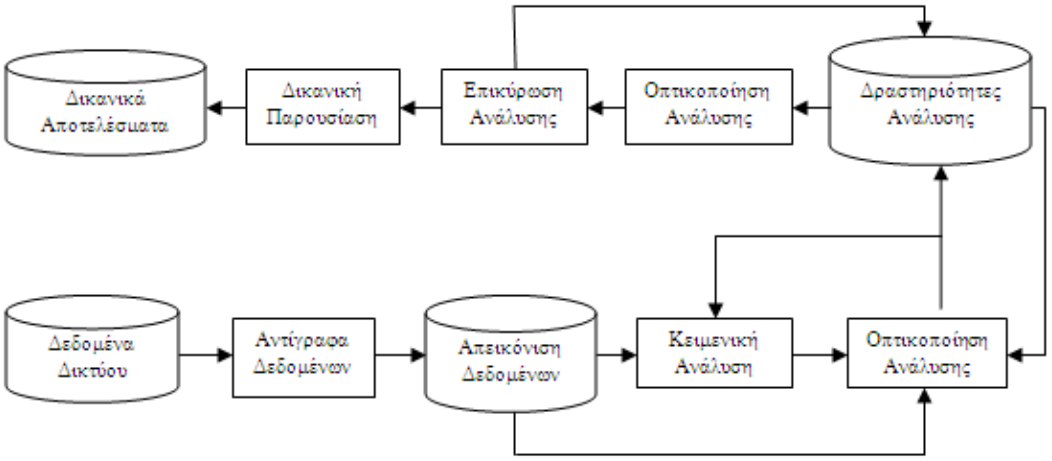
Εικόνα 2.8.Β. Παράλληλο Δικανικό Μοντέλο – Διαδικασία PSFP

2.3.6 Ένα μοντέλο Δικανικής Δικτύων με τεχνικές οπτικοποίησης

Η συλλογή δεδομένων από το δίκτυο, είναι ένα βασικό κομμάτι της Δικανικής Δικτύων. Ωστόσο, οι τρέχουσες δυνατότητες της ανάλυσης, αδυνατούν να ανταπεξέλθουν αποδοτικά όταν υπάρχει μεγάλος όγκος δεδομένων προς ανάλυση. Υπάρχει ανάγκη, για νέες δυνατότητες, που να επιτρέπουν τη γρηγορότερη εξέταση αυτών των δεδομένων. Η τεχνική της οπτικοποίησης έχει ως στόχο, να βελτιώσει τη διαδικασία της ανάλυσης. Η χρήση μόνο εκφράσεων και προτύπων αναζήτησης, δεν μπορούν να μειώσουν σε σημαντικό βαθμό την προσπάθεια που απαιτείται από τον αναλυτή για το φιλτράρισμα των προς ανάλυση δεδομένων. Μέσω της οπτικοποίησης επιτυγχάνεται μεγαλύτερη κατανόηση των δεδομένων της ανάλυσης αλλά και μεγαλύτερη ταχύτητα στην ίδια τη διαδικασία της ανάλυσης.

Το παρακάτω μοντέλο των Robert F. Erbacher, Kim Christiansen και Amanda Sundberg, προτείνει την εισαγωγή τεχνικών οπτικοποίησης (visualization) στο

ρεπερτόριο της ανάλυσης των δεδομένων του δικτύου [Erb06]. Σημαντικό ρόλο στην οπτικοποίηση παίζει και η αλληλεπίδραση με βρόχους ανατροφοδότησης.



Εικόνα 2.9. Διάγραμμα δικανικής δικτύων με την τεχνική της οπτικοποίησης

1. **Επικύρωση δεδομένων.** Τα δεδομένα από τις αρχικές πηγές δεδομένων πρέπει να προστατευθούν ώστε να διασφαλιστεί η εγκυρότητα τους και να παρέχεται η δυνατότητα επαλήθευσης. Να είναι δυνατό δηλαδή, να αποδειχθεί, ότι τα δεδομένα δεν έχουν αλλαχθεί από την στιγμή που συλλέχθηκαν. Αυτό μπορεί να γίνει είτε με την κρυπτογράφηση των δεδομένων είτε κάνοντας αντίγραφα τους σε ξεχωριστούς σκληρούς δίσκους.

2. **Ανάλυση κειμενικής βάσης (text-based).** Οι θεμελιώδεις δυνατότητες της ανάλυσης των δεδομένων, της δικτυακής κίνησης, βασίζονται, στην ανάλυση της κειμενικής αναπαράστασης (textual representation), των δικτυακών δεδομένων και στην αντιστοίχιση τους με πρότυπα δυαδικής βάσης (binary-based). Το αρχικό σημείο εστίασης της ανάλυσης, είναι η πραγματοποίηση φιλτραρίσματος, ώστε να απομείνουν μόνο οι πληροφορίες που παρουσιάζουν ενδιαφέρον στην εκάστοτε περίπτωση. Στη συνέχεια της ανάλυσης και αφού έχουν γίνει γνωστές περισσότερες πληροφορίες, το ενδιαφέρον στρέφεται ξανά προς τα πρωτογενή-ανεπεξέργαστα δεδομένα (raw data), ώστε να ανακαλυφθούν άλλα

συστήματα που έχουν γίνει στόχοι της ίδιας επίθεσης. Δεδομένου ότι το φιλτράρισμα των δεδομένων, ώστε να περιοριστεί το πεδίο εστίασης της ανάλυσης, είναι υψίστης σημασίας, κάποιες επιπλέον ικανότητες ανάλυσης, όπως οι παρακάτω, είναι απαραίτητες.

- **Αντιστοίχιση προτύπων.** Για την αναγνώριση της ακολουθίας των δραστηριοτήτων μιας επίθεσης, είναι σημαντική η αναζήτηση προτύπων της δραστηριότητας, με σταθερές ή κανονικές εκφράσεις. Όπως για παράδειγμα η αναζήτηση ακολουθιών από bytes, σε γνωστές επιθέσεις υπερχείλισης της μνήμης.

- **Αναγνώριση ροής.** Η ικανότητα ομαδοποίησης πακέτων μπορεί να μειώσει σε σημαντικό βαθμό το φόρτο εργασίας. Η πιο σημαντική παράμετρος ομαδοποίησης βασίζεται στις ροές συμβάντων (event streams). Συσχετίζοντας τα πακέτα με τις ροές συμβάντων, μπορεί γρήγορα να μειωθεί ένας μεγάλος αριθμός πακέτων μιας ροής, εφόσον η ροή αυτή δεν θεωρηθεί επικίνδυνη.

- **Εξέταση δεδομένων.** Στο τελικό στάδιο της ανάλυσης, θα χρειαστεί να εξεταστούν τα ανεπεξέργαστα πακέτα δεδομένων (raw data), σε δυαδική, κειμενική (textual) ή υβριδική (hybrid) μορφή, ώστε να ανακαλυφθούν ποια πακέτα σχετίζονται με την επίθεση και πως αυτή υποκινήθηκε.

- **Γνώση του τομέα (domain).** Για την ανάλυση των δικτυακών δεδομένων, ο αναλυτής πρέπει να έχει εμπειρία και να μπορεί να κατανοεί τα δεδομένα του δικτύου, ώστε να μπορέσει να προσδιορίσει αν τα πακέτα είναι κακόβουλα ή όχι. Επίσης η γνώση του τοπικού δικτύου και της πολιτικής ασφαλείας που εφαρμόζεται, βοηθούν στην αναγνώριση μιας ακολουθίας πακέτων ως επικίνδυνη.

3. **Οπτικοποιημένη ανάλυση.** Η διαδικασία της ανάλυσης δυσκολεύει και γίνεται πολύ αργή, λόγω του μεγάλου όγκου των δεδομένων. Η τεχνική της οπτικοποίησης έχει ως στόχο να βελτιώσει τη διαδικασία της ανάλυσης,

καθώς είναι σχεδιασμένη να λειτουργεί σε συνεργασία με τις παραδοσιακές δυνατότητες ανάλυσης. Η οπτικοποιημένη ανάλυση βασίζεται στα ακατέργαστα δεδομένα (raw data) αλλά και στα αποτελέσματα των παραδοσιακών τεχνικών. Αυτό δημιουργεί ένα αλληλεπιδραστικό βρόχο ανάδρασης, στον οποίο η κειμενική ανάλυση (text based) παρέχει ένα εννοιολογικό πλαίσιο το οποίο ενσωματώνεται στην οπτικοποίηση. Η οπτικοποίηση στοχεύει στην καλύτερη κατανόηση των αποτελεσμάτων, κάνοντας παράλληλα πιο αποδοτική και πιο αποτελεσματική την ανάλυση.

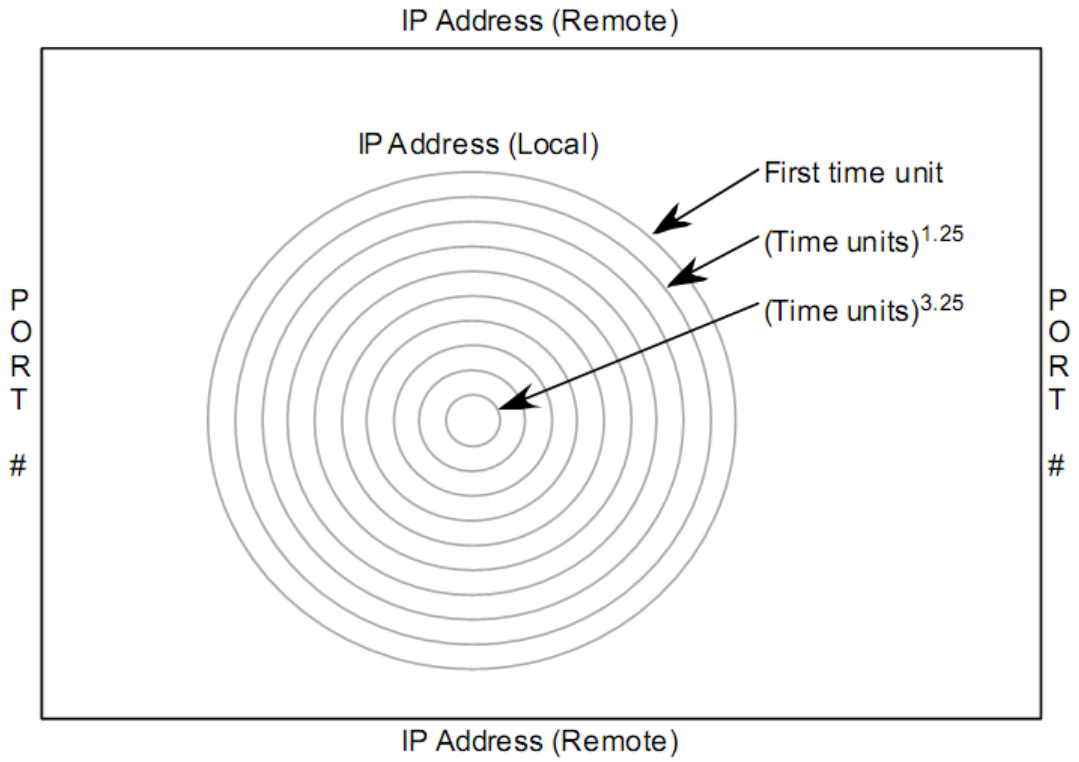
4. **Αποτελέσματα της ανάλυσης.** Τυπικά, η βασική πτυχή της ανάλυσης είναι τα αποτελέσματα της. Ωστόσο, σε αυτό το μοντέλο, η ίδια η διαδικασία της ανάλυσης έχει ιδιαίτερη σημασία, καθώς τα αποτελέσματα της χρησιμεύουν ως είσοδος σε ένα δεύτερο αλληλεπιδραστικό βρόχο ανάδρασης, ο οποίος στοχεύει σε μελλοντική ανάλυση και στην νομική αποδοχή των αποτελεσμάτων. Στόχος είναι να καταγραφούν οι ενέργειες του αναλυτή σε μια βάση δεδομένων, για μελλοντική ανάλυση, ώστε το σύνολο των δραστηριοτήτων να παρέχει μια εικόνα της διαδικασίας της ανάλυσης. Για παράδειγμα, η ανάπτυξη τεχνικών μηχανικής μάθησης, οι οποίες θα καθοδηγήσουν την ανάλυση, αναγνωρίζοντας τυπικές δραστηριότητες προηγούμενων αναλύσεων, οι οποίες αποδείχτηκαν επιτυχημένες. Η βάση δεδομένων θα παρέχει το ιστορικό των δραστηριοτήτων που πραγματοποιήθηκαν.

5. **Οπτικοποίηση της ανάλυσης και επικύρωση.** Καθώς τα δεδομένα από την διαδικασία της ανάλυσης έχουν συλλεχθεί , είναι απαραίτητη η ανάλυση των ίδιων των δεδομένων. Για την παρουσίαση αυτών των δεδομένων ίσως χρειαστούν επιπλέον τεχνικές οπτικοποίησης. Τα δεδομένα αυτά θα αποκαλύψουν ποιες τεχνικές ανάλυσης ή διαδικασίες, φαίνεται να είναι πιο αποδοτικές. Επίσης, θα αποκαλύπτει ποιες τεχνικές λείπουν ή δεν χρησιμοποιούνται αποδοτικά. Οι τεχνικές αυτές θα εφαρμόζονται στα δεδομένα που προήλθαν από την ανάλυση, εστιάζοντας στην επικύρωση και την παρουσίαση τους.

2.3.6.1 Η οπτικοποίηση στην Ανάλυση

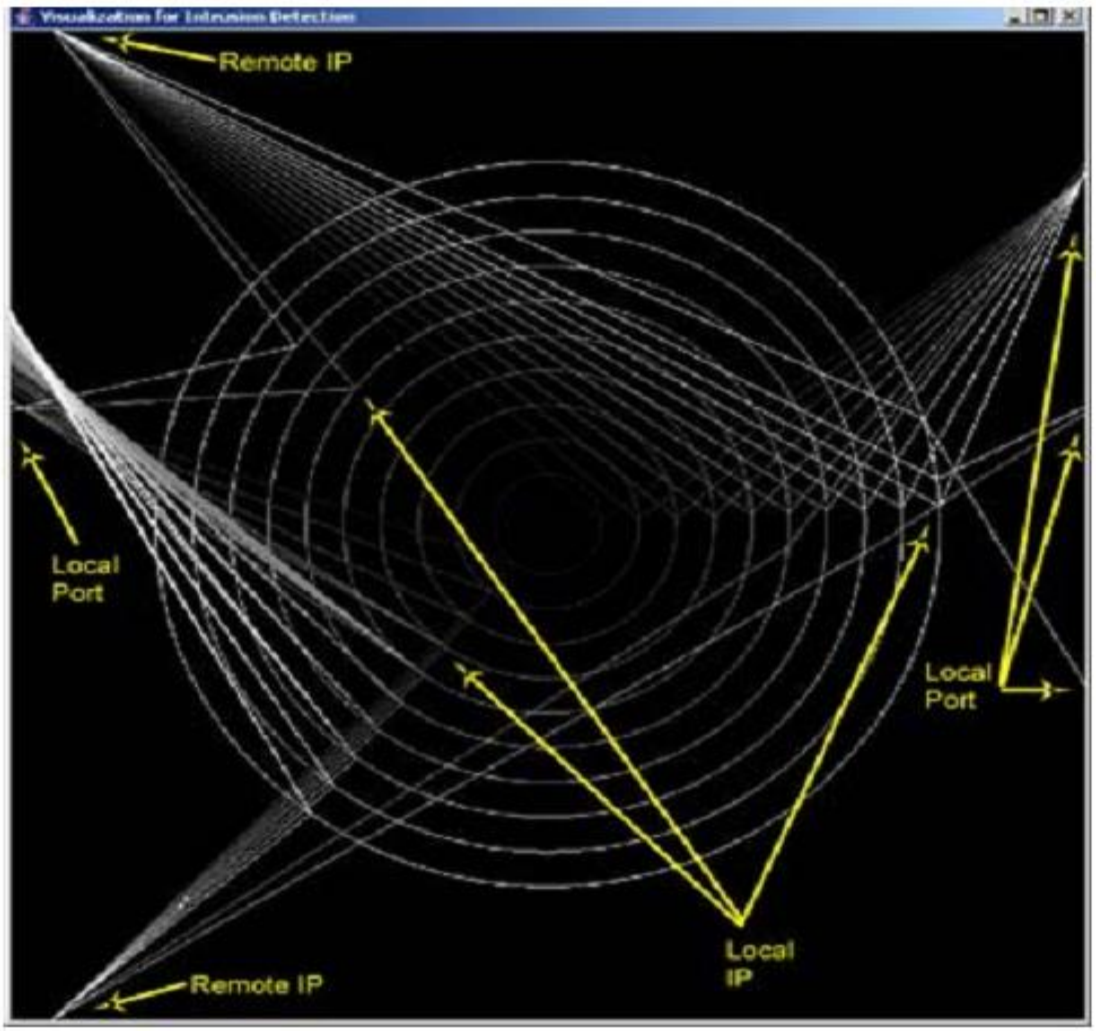
Οι τεχνικές οπτικοποίησης σε συνδυασμό με τις τεχνικές αλληλεπίδρασης, μπορούν σε μεγάλο βαθμό να προσδώσουν ταχύτητα στην ανάλυση. Κάποια τεχνική μπορεί να είναι περισσότερο κατάλληλη από κάποια άλλη για ένα συγκεκριμένο πρόβλημα. Ένα χρήσιμο χαρακτηριστικό είναι η δυνατότητα πολλαπλών οπτικών όψεων από διαφορετικές τεχνικές οπτικοποίησης, πάνω στα ίδια δεδομένα, με χρήση διαφορετικών παραμέτρων. Ένα επίσης χρήσιμο χαρακτηριστικό, είναι η αλληλεπίδραση των τεχνικών. Όταν οι παράμετροι αλλάζουν σε μια τεχνική, τότε η αλλαγή μεταφέρεται και στις υπόλοιπες.

Οι τεχνικές οπτικοποίησης βασίζονται σε πολλές παραμέτρους, όπως ο αριθμός πόρτας , οι διευθύνσεις IP προέλευσης και προορισμού, το μέγεθος των πακέτων και άλλα. Η βασικά τεχνική οπτικοποίησης αφορά την αναπαράσταση της κίνησης του δικτύου με αποτελεσματικό τρόπο, παρουσιάζοντας όσο το δυνατόν περισσότερα δεδομένα. Καταρχήν η τεχνική παρουσιάζει (Εικόνα 2.10) την τοπική διεύθυνση IP μιας σύνδεσης και γύρω από αυτήν μια συστοιχία κύκλων, οι οποίοι αναπαριστούν τα δεδομένα. Όσο μεγαλύτερη ακτίνα έχει ο κύκλος τόσο πιο πρόσφατα είναι τα δεδομένα που αναπαριστά. Επίσης απεικονίζεται η απομακρυσμένη διεύθυνση IP (ενός ή περισσότερων υπολογιστών).



Εικόνα 1.10. Απεικόνιση των διευθύνσεων IP

Στην εικόνα 2.11, απεικονίζεται η τεχνική οπτικοποίησης εφαρμοσμένη στα δεδομένα του δικτύου. Οι κύκλοι που αναπαριστούν τα παλαιότερα δεδομένα, έχουν μικρότερη ακτίνα και φαίνονται ξεθωριασμένοι, δείχνοντας έτσι ότι πρέπει να έχουν μικρότερη επίδραση στην ανάλυση, διατηρώντας όμως την πληροφορία για τον αναλυτή. Επίσης, στην εικόνα φαίνεται η συνεχής δραστηριότητα από πολλούς απομακρυσμένους υπολογιστές. Η οπτικοποίηση σχεδιάστηκε για να παρουσιάζει σε ένα πρώτο στάδιο τα βασικά χαρακτηριστικά των δεδομένων, καθώς και τις μεταξύ τους συσχετίσεις. Μετά από αυτό το πρώτο στάδιο φιλτραρίσματος, η ανάλυση απαιτεί περισσότερες δυνατότητες, λεπτομερέστερης εξέτασης, πέρα από αυτή που παρέχει η οπτικοποίηση.



Εικόνα 2.11. Απεικόνιση της τεχνικής οπτικοποίησης

ΚΕΦΑΛΑΙΟ 3

Εργαλεία και τεχνικές υποστήριξης

Το παρόν κεφάλαιο παρουσιάζει τα πιο συχνά χρησιμοποιούμενα εργαλεία για την υποστήριξη της δικανικής δικτύων. Όλα τα εργαλεία που παρουσιάζονται, είναι λογισμικό ανοιχτού κώδικα (open source). Ωστόσο, υπάρχουν και άλλα εμπορικά εργαλεία, όπως το NetIntercept, το NetWitness και το Carnivore που χρησιμοποιήθηκε από το FBI. Ο συνδυασμός δύο ή περισσότερων εργαλείων δίνει την δυνατότητα για συλλογή και φιλτράρισμα των πακέτων, την ανάλυση καταγεγραμμένων αρχείων (log files), την ανακατασκευή ροών δεδομένων, τη συσχέτιση δεδομένων από διαφορετικές πηγές, την εμφάνιση λεπτομερειών σε επίπεδο εφαρμογής και άλλες εξειδικευμένες λειτουργίες.

3.1 Τι είναι packet sniffer

Ο packet sniffer είναι ένα εργαλείο (software ή hardware), το οποίο συλλέγει δεδομένα που μεταδίδονται σε ένα δίκτυο και προσπαθεί να εμφανίσει τα δεδομένα των πακέτων με όσο το δυνατόν μεγαλύτερη λεπτομέρεια. Οι packet sniffers είναι επίσης γνωστοί και ως network analyzers ή protocol analyzers. Σε ένα τυπικό δίκτυο, ο κάθε υπολογιστής δέχεται μόνο τα πακέτα δεδομένων που προορίζονται για αυτόν. Τα πακέτα που προέρχονται από ή προορίζονται για τους γειτονικούς υπολογιστές, τα βλέπει αλλά τα απορρίπτει. Ο packet sniffer αναγκάζει τον υπολογιστή και συγκεκριμένα την NIC (Network Interface Card), να αρχίσει να προσέχει και αυτά τα πακέτα, τα οποία προορίζονται για άλλους υπολογιστές. Για να το καταφέρει αυτό θέτει τη NIC σε ειδική λειτουργία, γνωστή ως promiscuous mode. Όταν η NIC βρίσκεται σε αυτή τη λειτουργία, ένα μηχάνημα μπορεί να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του. Ο ίδιος ο packet sniffer είναι παθητικός. Παρατηρεί τα μηνύματα που στέλνονται και

λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που τρέχουν στον υπολογιστή αλλά ο ίδιος δεν στέλνει ποτέ πακέτα.

Ο packet sniffer μπορεί να λειτουργήσει σε περιβάλλον όπου όλοι οι υπολογιστές είναι συνδεδεμένοι στον ίδιο δίαυλο με χρήση συσκευής hub (shared Ethernet) και βλέπουν τα πακέτα που προορίζονται προς όλους τους υπολογιστές. Στην περίπτωση όπου οι υπολογιστές συνδέονται σε switch αντί σε hub (switched Ethernet), οι υπολογιστές που λειτουργούν σε promiscuous mode δεν θα μπορέσουν να συλλέξουν τα ξένα πακέτα. Οι συσκευές switch διατηρούν ένα πίνακα ο οποίος περιέχει τις MAC διευθύνσεις όλων των υπολογιστών και τις πόρτες που συνδέονται σε αυτό. Έτσι κατευθύνει σε κάθε υπολογιστή μόνο τα πακέτα που προορίζονται προς αυτόν.

Υπάρχουν τρείς βασικές μέθοδοι sniffing: IP-based, MAC-based και ARP-based [Spa03]. Κάποιες από αυτές τις τεχνικές μπορούν να λειτουργήσουν και σε περιβάλλον με switch.

- **IP-based.** Αυτή είναι η εξ' ορισμού μέθοδος πραγματοποίησης του packet sniffing. Λειτουργεί θέτοντας την κάρτα δικτύου σε promiscuous mode και συλλέγει όλα τα πακέτα που ταιριάζουν στο φίλτρο της διεύθυνσης IP. Συνήθως το φίλτρο των IP διευθύνσεων δεν είναι ενεργοποιημένο και έτσι συλλέγονται όλα τα πακέτα. Αυτή η μέθοδος μπορεί να λειτουργήσει μόνο σε δίκτυα που δεν χρησιμοποιείται switch ή αντίστοιχου επιπέδου συσκευή.

- **MAC-based.** Λειτουργεί θέτοντας την κάρτα δικτύου σε promiscuous mode και συλλέγει όλα τα πακέτα που ταιριάζουν στο φίλτρο της διεύθυνσης MAC. Μπορεί να λειτουργήσει μόνο σε δίκτυα που δεν χρησιμοποιείται switch ή αντίστοιχου επιπέδου συσκευή.

- **ARP-based.** Αυτή η μέθοδος δεν λειτουργεί με τον ίδιο τρόπο όπως οι δυο προηγούμενες. Δεν λειτουργεί δηλαδή, θέτοντας την κάρτα δικτύου σε promiscuous mode, αλλά δηλητηριάζοντας την ARP μνήμη (ARP poisoning) των υπολογιστών από τους οποίους θέλει να υποκλέψει πακέτα. Με αυτό τον τρόπο, οι υπολογιστές, δεν ανταλλάσουν απευθείας τα πακέτα, αλλά περνούν από ένα ενδιάμεσο υπολογιστή ο οποίος συλλέγει-αντιγράφει τα

πακέτα και στη συνέχεια τα στέλνει στον τελικό προορισμό τους (man in the middle attack). Αυτή η τεχνική μπορεί να λειτουργήσει και σε δίκτυα όπου υπάρχουν συσκευές switch.

Ένας packet sniffer αποτελείται από δυο μέρη: τη βιβλιοθήκη σύλληψης πακέτων (packet capture library) και τον αναλυτή πακέτων (packet analyzer) [E34]. Η βιβλιοθήκη σύλληψης πακέτων λαμβάνει ένα αντίγραφο κάθε πλαισίου επιπέδου ζεύξης (data link layer) που στέλνεται ή λαμβάνεται από τον υπολογιστή. Τα μηνύματα που ανταλλάσσονται από τα πρωτόκολλα ανώτερων επιπέδων, όπως το HTTP, FTP, TCP, UDP ή το IP, τελικά ενθυλακώνονται όλα μέσα σε πλαίσια επιπέδου ζεύξης τα οποία μεταδίδονται μέσω φυσικών μέσων όπως ένα καλώδιο Ethernet. Επομένως, η σύλληψη όλων των πλαισίων επιπέδου ζεύξης παρέχει όλα τα μηνύματα που στέλνονται και λαμβάνονται από όλα τα πρωτόκολλα και όλες τις εφαρμογές που εκτελούνται.

Το δεύτερο συστατικό στοιχείο, είναι ο αναλυτής πακέτων, ο οποίος απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο μήνυμα ενός πρωτοκόλλου. Για το σκοπό αυτό, ο αναλυτής πακέτων πρέπει να "καταλαβαίνει" τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα. Για παράδειγμα, η απεικόνιση των διαφόρων πεδίων, των μηνυμάτων που ανταλλάσσονται χρησιμοποιώντας το πρωτόκολλο HTTP έχει ως εξής: Ο αναλυτής πακέτων καταλαβαίνει τη μορφή των πλαισίων Ethernet και επομένως μπορεί να αναγνωρίσει ένα αυτοδύναμο πακέτο IP (IP datagram) μέσα σε ένα πλαίσιο Ethernet. Επίσης, καταλαβαίνει τη μορφή ενός IP datagram, ώστε να είναι σε θέση να εξάγει ένα TCP segment που περιέχεται μέσα σε ένα IP datagram. Επιπλέον, καταλαβαίνει τη δομή ενός TCP segment οπότε μπορεί να εξάγει το μήνυμα HTTP που περιέχεται στο TCP segment. Τέλος, καταλαβαίνει το πρωτόκολλο HTTP και έτσι, για παράδειγμα, γνωρίζει ότι τα πρώτα bytes ενός μηνύματος HTTP θα περιέχουν τις ακολουθίες χαρακτήρων "GET", "POST" ή "HEAD".

3.2 Εργαλεία υποστήριξης

3.2.1 Tcpdump- WinDump

Το Tcpdump είναι ένα εργαλείο που χρησιμοποιείται για να συλλέξει πακέτα δεδομένων τα οποία μεταδίδονται στο δίκτυο στο οποίο είναι συνδεδεμένος ο υπολογιστής και για την ανάλυση των πακέτων. Εκτελείται από τη γραμμή εντολών, αποκρυπτογραφεί τα bits και τα εμφανίζει σε μια αναγνώσιμη για τον άνθρωπο μορφή. Το Tcpdump προορίζεται για χρήση σε UNIX-συμβατά λειτουργικά συστήματα και χρησιμοποιεί τη βιβλιοθήκη libpcap για να συλλέγει πακέτα. Η αντίστοιχη έκδοση για Windows είναι το WinDump, το οποίο χρησιμοποιεί την αντίστοιχη βιβλιοθήκη WinPcap. [E31, E32]

Για την εγκατάσταση τους απαιτείται να έχει εγκατασταθεί νωρίτερα η αντίστοιχη βιβλιοθήκη libPCAP / WinPCAP. Το Tcpdump εμφανίζει την κεφαλίδα των πακέτων που συλλέγει από το δίκτυο μέσω κάποιου interface. Η σύνταξη του Tcpdump (ισχύει και για το WinDump) έχει ως εξής [E319]:

tcpdump [*επιλογές*] [*φίλτρο*]

Μερικές από τις βασικές επιλογές του Tcpdump:

[-c count]: Σταματάει να συλλέγει πακέτα μόλις συλλέξει το πλήθος πακέτων που καθορίζεται από την τιμή του count.

[-C file_size]: Προτού αποθηκευθεί ένα πακέτο σε ένα αρχείο, ελέγχει αν το πακέτο έχει μικρότερο μέγεθος από αυτό που καθορίζεται στο file_size.

[-F file]: Χρησιμοποιεί ένα αρχείο (που καθορίζεται στο file) ως είσοδο για την έκφραση φιλτραρίσματος (filter expression).

[-i interface]: Υποδεικνύεται πιο interface θα χρησιμοποιηθεί για τη σύλληψη πακέτων.

[-w file]: Αποθηκεύει τα πακέτα που συλλέγονται στο αρχείο με όνομα file.

Παραδείγματα φίλτρων:

tcpdump "udp" - Μόνο τα UDP πακέτα

tcpdump "udp dst port 53" - Μόνο DNS requests (προορίζονται για την πόρτα 53)

tcpdump "src host mail.google.com" - Μόνο τα πακέτα από το mail.google.com

Μορφή της εξόδου (output) από το TcpDump

Η μορφή που θα έχουν τα αποτελέσματα στην έξοδο του TcpDump, εξαρτάται από το πρωτόκολλο. Για παράδειγμα στα TCP πακέτα η έξοδος έχει την εξής μορφή:

src > dst: flags data-seqno ack window urgent options

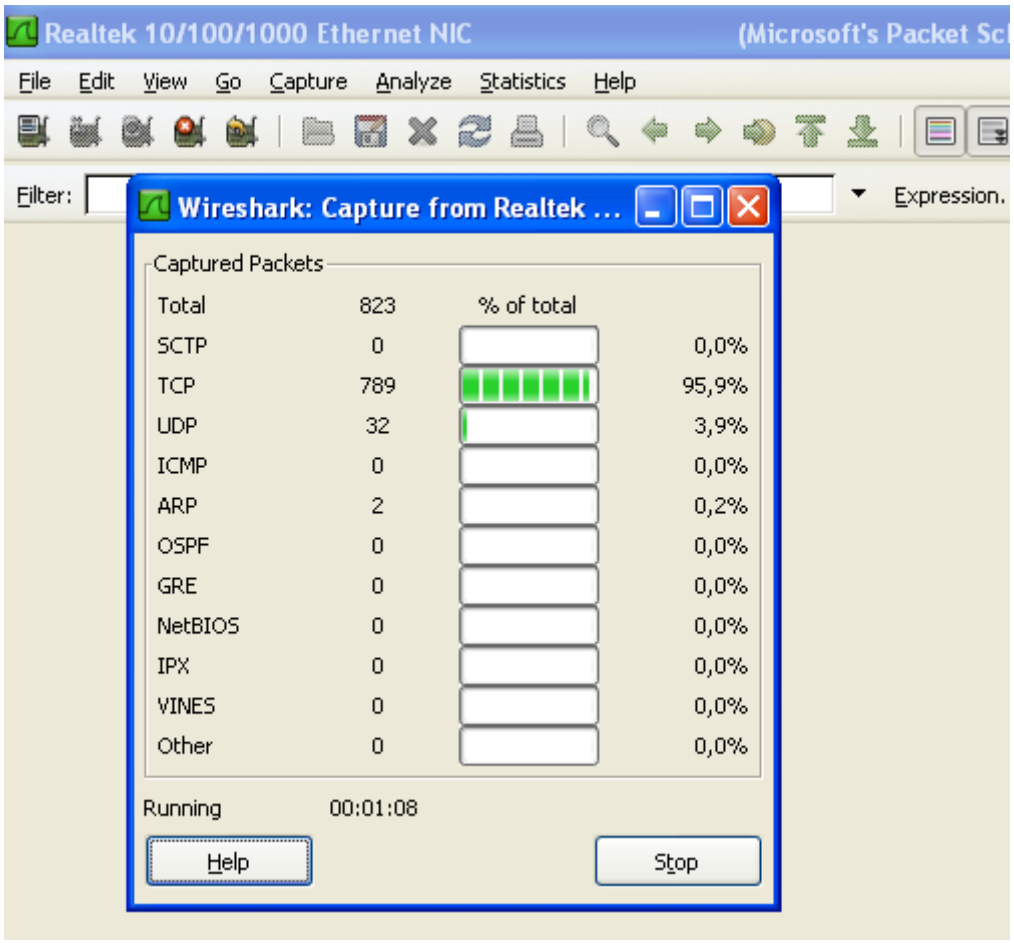
Τα src και dst, δηλώνουν τις διευθύνσεις IP και τις πόρτες προέλευσης και προορισμού. Το flags είναι ένα ή περισσότερα flags του TCP πρωτοκόλλου, όπως S (SYN), F (FIN), P (PUSH), R (RST) ή τελεία όταν δεν υπάρχει κανένα flag. Το data-seqno, περιγράφει το τμήμα του συνεχόμενου χώρου που καταλαμβάνουν τα δεδομένα. Ack είναι ο αριθμός ακολουθίας των επόμενων δεδομένων που αναμένονται από την άλλη άκρη της σύνδεσης. Window είναι ο αριθμός των bytes, του διαθέσιμου χώρου λήψης, στην άλλη πλευρά της σύνδεσης. Το urgent δηλώνει αν το πακέτο περιλαμβάνει επείγοντα δεδομένα. Τέλος το options περιλαμβάνει επιλογές του TCP.

3.2.2 Wireshark – Ethereal

Wireshark (αρχικά ονομαζόταν Ethereal) είναι ένας packet analyzer παρόμοιος με το Tcpdump, ο οποίος όμως έχει γραφικό περιβάλλον, παρέχει περισσότερες πληροφορίες και επιλογές για ταξινόμηση και φιλτράρισμα των πακέτων. Επιτρέπει στο χρήστη να παρακολουθήσει όλη την κίνηση που περνά από το δίκτυο και μπορεί να εκτελεστεί σε διάφορα λειτουργικά συστήματα, όπως Linux,

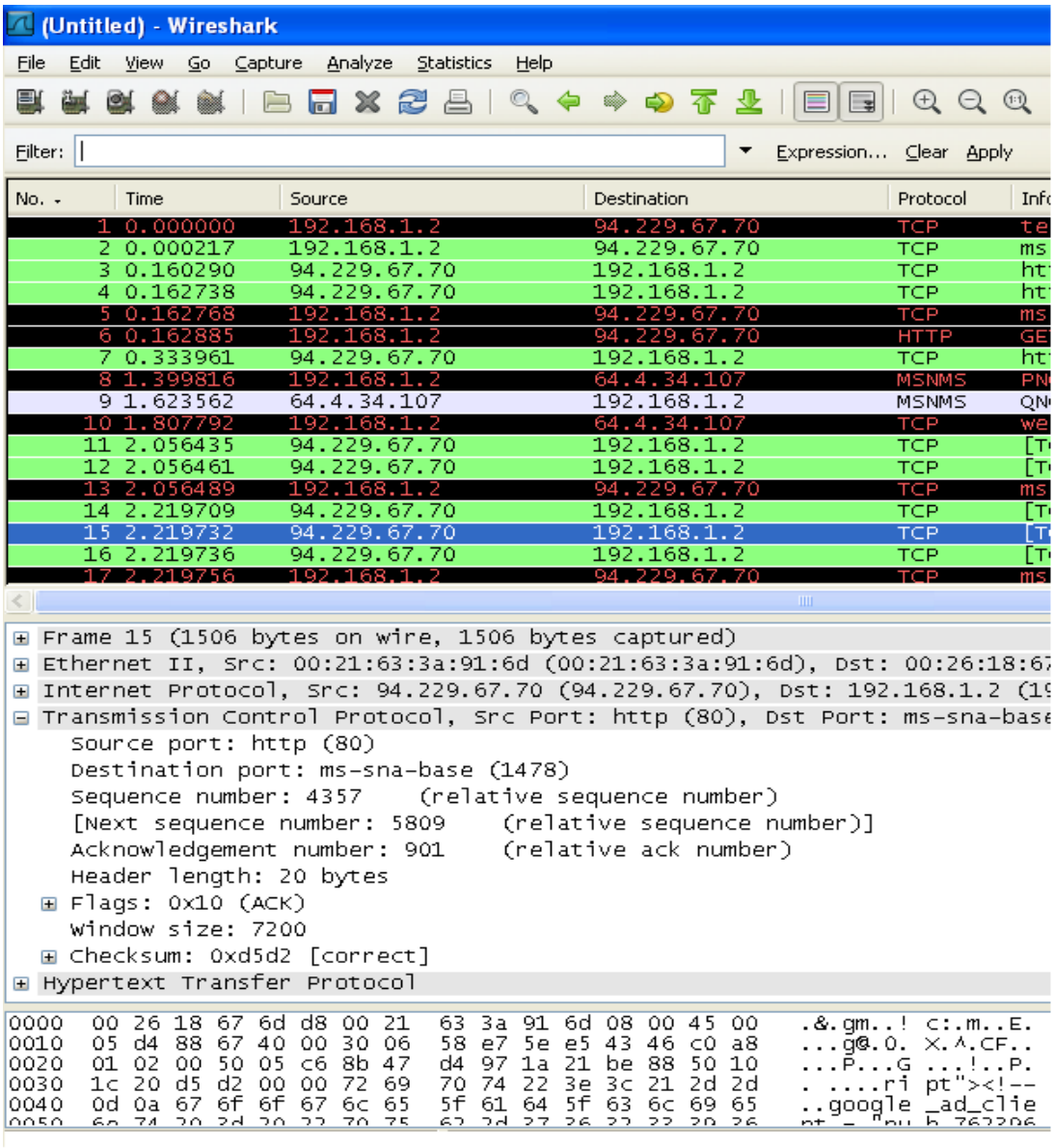
Mac OS X και Microsoft Windows. Το Wireshark καταλαβαίνει τη δομή διαφόρων δικτυακών πρωτοκόλλων και μπορεί να εμφανίσει την ενθυλάκωση και τα πεδία πακέτων με διαφορετικά πρωτόκολλα δικτύου. Για τη σύλληψη πακέτων χρησιμοποιεί το pcap και μπορεί να συλλέξει πακέτα απευθείας από ένα ενεργό δίκτυο ή από αρχεία τα οποία περιέχουν πακέτα από προηγούμενη συλλογή. Επειδή υποστηρίζει τη μορφή των αρχείων του libpcap, μπορεί να διαβάσει αρχεία από το Tcpdump ή άλλες εφαρμογές που υποστηρίζουν αυτή τη μορφή (format). [E33, E34]

Η διαδικασία σύλληψης πακέτων με το Wireshark είναι απλή και άμεση. Αφού εκτελεστεί το λογισμικό Wireshark, εμφανίζεται το αρχικό μενού από όπου επιλέγοντας Capture → Interfaces ανοίγει ένα νέο παράθυρο, το οποίο περιέχει όλα τα interfaces, από τα οποία μπορεί να γίνει σύλληψη πακέτων. Συνήθως υπάρχει μονό ένα interface εκτός και αν υπάρχουν περισσότερες κάρτες δικτύου στο υπολογιστή. Στην τελευταία περίπτωση πρέπει να επιλεγεί μόνο ένα interface από το οποίο θα συλλέγονται τα πακέτα. Από το κουμπί Options δίπλα από το αντίστοιχο interface, μπορούν να γίνουν κάποιες επιλογές για τη σύλληψη των πακέτων σε αυτό το interface , όπως να εφαρμοστεί κάποιο φίλτρο καθώς συλλέγονται τα πακέτα, να προσδιοριστεί το χρονικό διάστημα για το οποίο θα γίνεται σύλληψη των πακέτων ή το μέγιστο συνολικό μέγεθος των πακέτων που θα συλλεχθούν. Αφού γίνουν όλες οι επιθυμητές ρυθμίσεις, πατώντας το κουμπί Start ξεκινά η σύλληψη των πακέτων που στέλνονται ή λαμβάνονται από τον υπολογιστή, στο αντίστοιχο interface. Στην εικόνα 3.1 φαίνεται το παράθυρο που συνοψίζει τον αριθμό των διαφόρων ειδών πακέτων που συλλαμβάνονται και περιέχει το κουμπί Stop, από το οποίο μπορεί να διακοπή η σύλληψη πακέτων.



Εικόνα 3.1. Στιγμιότυπο του Wireshark

Επιλέγοντας stop θα έχει ως αποτέλεσμα να εξαφανισθεί το παράθυρο capture του Wireshark και το κύριο παράθυρο του Wireshark να εμφανίσει όλα τα πακέτα που συνελήφθησαν από τότε που άρχισε η σύλληψη πακέτων.



Εικόνα 3.2. Η διεπαφή του Wireshark

Στην εικόνα 3.2 φαίνεται η διεπαφή του Wireshark, η οποία περιλαμβάνει πέντε κύρια συστατικά στοιχεία:

1. Τα **μενού των εντολών** (command menus) που βρίσκονται στο επάνω μέρος του παραθύρου.

2. Το **πεδίο του φίλτρου παρουσίασης πακέτων** (packet display filter field) στο οποίο μπορεί να γίνει φιλτράρισμα των πληροφοριών που θα εμφανίζονται στο παράθυρο καταλόγου πακέτων (και επομένως στα παράθυρα λεπτομερειών επικεφαλίδας και περιεχομένων πακέτου). Το

φίλτρο απαιτεί την εισαγωγή του ονόματος ενός πρωτοκόλλου ή κάποια άλλη πληροφορία ώστε να φιλτραριστεί η πληροφορία που θα παρουσιαστεί. Για παράδειγμα εισάγοντας στο πεδίο το πρωτόκολλο HTTP, το Wireshark θα αποκρύψει όλα τα πακέτα εκτός από εκείνα που αντιστοιχούν σε μηνύματα HTTP.

3. Το **παράθυρο καταλόγου πακέτων** (packet-listing window), το οποίο παρουσιάζει περίληψη της μιας γραμμής, για κάθε πακέτο που συλλαμβάνεται, η οποία περιλαμβάνει τον αριθμό πακέτου (πρόκειται για αριθμό που απονέμεται από το Wireshark), τον χρόνο σύλληψης του πακέτου, τις διευθύνσεις πηγής και προορισμού του πακέτου, το είδος του πρωτοκόλλου και πληροφορίες σχετικά με το πρωτόκολλο. Ο κατάλογος των πακέτων μπορεί να ταξινομηθεί σύμφωνα με οποιαδήποτε από αυτές τις κατηγορίες κάνοντας κλικ στο όνομα της αντίστοιχης στήλης. Στο πεδίο είδος πρωτοκόλλου (protocol type) αναφέρεται το ανωτάτου επιπέδου πρωτόκολλο το οποίο έστειλε ή έλαβε ένα πακέτο, δηλαδή, το πρωτόκολλο που είναι η πηγή ή ο τελικός αποδέκτης αυτού του πακέτου.

4. Το **παράθυρο λεπτομερειών επικεφαλίδας πακέτου** (packet- header details window) παρέχει λεπτομέρειες σχετικά με το επιλεγμένο στο παράθυρο packet-listing πακέτο. Οι λεπτομέρειες αυτές περιλαμβάνουν πληροφορίες σχετικά με το πλαίσιο Ethernet και το IP datagram που περιέχουν αυτό το πακέτο. Εάν το πακέτο έχει μμεταφερθεί με TCP ή UDP, θα παρουσιαστούν και οι λεπτομέρειες που αφορούν το TCP ή το UDP. Τέλος, λεπτομέρειες παρέχονται επίσης για το ανωτάτου επιπέδου πρωτόκολλο το οποίο έστειλε ή έλαβε αυτό το πακέτο.

5. Το **παράθυρο περιεχομένων πακέτου** (packet-contents window) παρουσιάζει ολόκληρο το περιεχόμενο ενός πλαισίου σε μορφή ASCII και σε δεκαεξαδική μορφή.

3.2.3 Kismet

Το Kismet είναι ένας ανιχνευτής δικτύου, packet sniffer και IDS, για 802.11 (802.11a, 802.11b και 802.11g) ασύρματα τοπικά δίκτυα. Μπορεί να λειτουργήσει σε λειτουργικά συστήματα Windows και UNIX με οποιαδήποτε ασύρματη κάρτα δικτύου που υποστηρίζει τη λειτουργία ”raw monitoring mode” (rfmon). Το Kismet λειτουργεί παθητικά, δηλαδή συλλέγει πακέτα από το δίκτυο χωρίς όμως το ίδιο να στέλνει και μπορεί να ανιχνεύσει ασύρματα σημεία πρόσβασης (ακόμα και αυτά που έχουν κρυμμένο το SSID τους). Έχει τη δυνατότητα να καταγράφει τα πακέτα που συλλέγει και να τα αποθηκεύει σε μορφή συμβατή με τα tcpdump/Wireshark. Επίσης μπορεί να ανακαλύψει το εύρος των IP διευθύνσεων που χρησιμοποιούνται από το ασύρματο δίκτυο. Για να ανιχνεύσει τα ασύρματα δίκτυα το Kismet χρησιμοποιεί την τεχνική της αναπήδησης καναλιών (channel-hopping), αλλάζει δηλαδή συνεχώς το κανάλι που παρακολουθεί, όχι όμως σειριακά. Το πλεονέκτημα της τεχνικής αυτής είναι ότι συλλέγει περισσότερα πακέτα επειδή τα γειτονικά κανάλια επικαλύπτονται. Το Kismet επίσης υποστηρίζει το γεωγραφικό προσδιορισμό των συντεταγμένων ενός δικτύου, αν χρησιμοποιηθεί επιπρόσθετα ένας GPS δέκτης [E35, E36].

3.2.4 Ngrep

Το Ngrep (network grep) αποτελεί μια προσαρμογή του grep από το UNIX, ώστε να μπορεί να παρακολουθεί την κίνηση του δικτύου. Βασίζεται στην βιβλιοθήκη libpcap και χρησιμοποιεί κανονικές ή δεκαεξαδικές εκφράσεις (hexadecimal expressions), οι οποίες εφαρμόζονται στο επίπεδο δικτύου (network layer), για να φιλτράρουν τη δικτυακή κίνηση. Υποστηρίζει IPv4/6, TCP, UDP, ICMPv4/6, IGMP, PPP, SLIP, FDDI και Token Ring. [E37, E38]

3.2.5 NetStumbler

Το NetStumbler είναι ένα εργαλείο, το οποίο διευκολύνει την ανίχνευση ασύρματων τοπικών δικτύων (WLAN) που χρησιμοποιούν τα πρότυπα 802.11a, 802.11b και 802.11g. Εκτελείται σε Windows λειτουργικά συστήματα και υπάρχει

διαθέσιμη έκδοση του MiniStumbler για Windows CE. Χρησιμοποιείται για να επιβεβαιώσει τις ρυθμίσεις του δικτύου, για να ανιχνεύσει τοποθεσίες του δικτύου με αδύναμο σήμα, να εντοπίσει τις αιτίες που προκαλούν παρεμβολές στο ασύρματο δίκτυο και να ανιχνεύσει μη πιστοποιημένα σημεία πρόσβασης. [E39] Το NetStumbler δεν έχει παθητική λειτουργία και για να μπορέσει να ανιχνεύσει ασύρματα σημεία πρόσβασης, εκπέμπει (broadcasts) αιτήσεις (requests) προς όλα τα ασύρματα σημεία που ανταποκρίνονται στο “ANY” ως αναγνωριστικό του SSID τους. Για αυτό το λόγο, τα ασύρματα σημεία που κρύβουν ή δεν εκπέμπουν το SSID τους, δεν μπορούν να ανιχνευθούν από το NetStumbler.

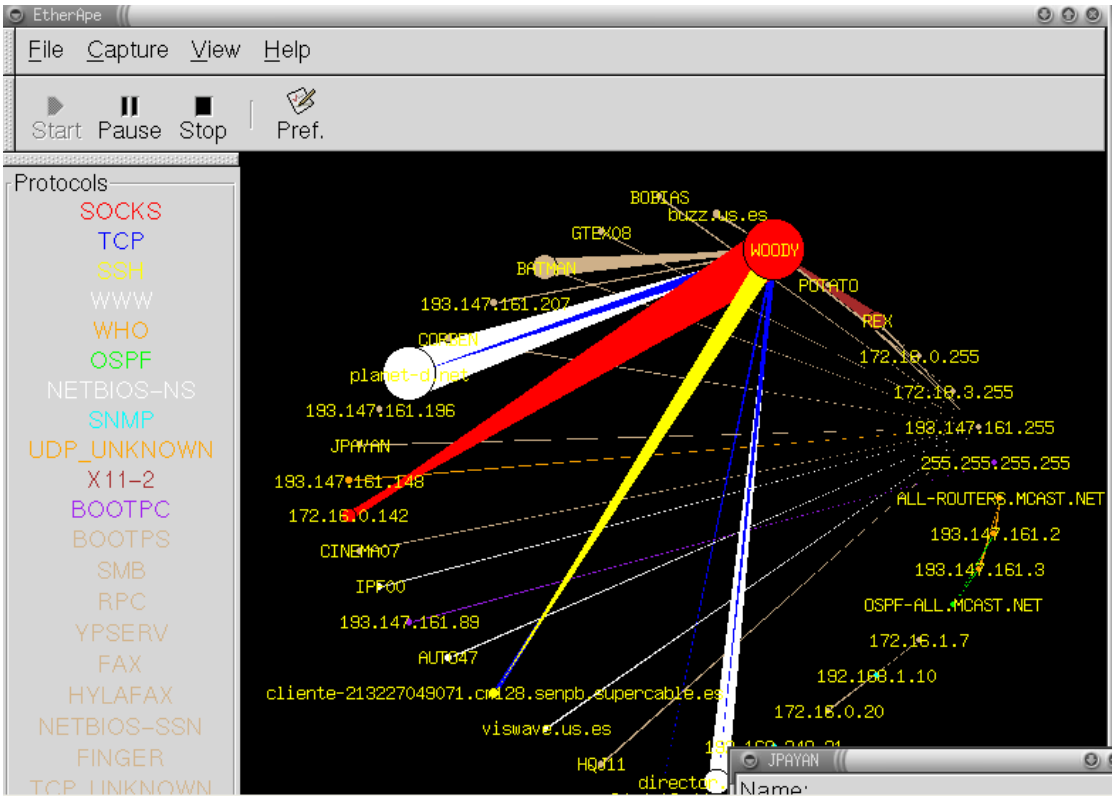
3.2.6 Argus

Το Argus είναι ένα εργαλείο παρακολούθησης (για χρήση σε περιβάλλον UNIX) των δραστηριοτήτων του δικτύου και ελέγχου των IP διευθύνσεων. Αποτελείται από δύο μέρη: το server, ο οποίος καταγράφει τη δικτυακή κίνηση που διέρχεται από μία ή περισσότερες NIC κάρτες του υπολογιστή και συναρμολογεί τις πληροφορίες που συνέλεξε σε δικτυακές ροές (network flows) και μια ομάδα από clients, οι οποίοι διαβάζουν τις ροές δεδομένων. Το Argus επεξεργάζεται πακέτα (είτε από αρχεία είτε κατευθείαν από το δίκτυο) και παράγει μια λεπτομερή αναφορά των ροών που ανίχνευσε. Οι αναφορές που παράγει το Argus περιέχουν όλες εκείνες τις σημαντικές πληροφορίες που είναι απαραίτητες για κάθε ροή, κρατώντας παράλληλα μικρό τον όγκο των δεδομένων, διευκολύνοντας την αποθήκευση, την επεξεργασία και την ανάλυση μεγαλύτερου όγκου δικτυακών δεδομένων σε μικρότερο χρονικό διάστημα [E310, E311].

3.2.7 EtherApe

Το EtherApe είναι ένας packet sniffer και συνάμα ένα εργαλείο παρακολούθησης της δικτυακής κίνησης, μέσα από γραφικό περιβάλλον, για χρήση σε περιβάλλον UNIX. Η δραστηριότητα του δικτύου παρουσιάζεται γραφικά, με κόμβους, οι οποίοι αποτελούν τους υπολογιστές του δικτύου και συνδέσμους μεταξύ αυτών. Οι κόμβοι και οι σύνδεσμοι που τους ενώνουν, φέρουν χρωματική κωδικοποίηση, η οποία αναπαριστά τα διαφορετικά πρωτόκολλα και τον όγκο της δικτυακής

κίνησης. Υποστηρίζει Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP και μπορεί επεξεργαστεί πακέτα είτε από αρχεία είτε κατευθείαν από το δίκτυο [E312, E313]. Στην εικόνα 3.3 φαίνεται η χρωματική αναπαράσταση των διαφόρων πρωτοκόλλων και το μέγεθος της κίνησης, ανάλογα με το μέγεθος της αντίστοιχης γραμμής.



Εικόνα 3.3. Χρωματική αναπαράσταση των πρωτοκόλλων με το EtherApe

3.2.8 Snort

Το Snort είναι δικτυακό εργαλείο (για χρήση σε περιβάλλον UNIX) ανίχνευσης και πρόληψης εισβολών (IDS/IPS), με δυνατότητες καταγραφής των πακέτων και ανάλυση της κίνησης, IP δικτύων σε πραγματικό χρόνο[E315].

Το Snort μπορεί να ρυθμιστεί ώστε λειτουργεί σε τέσσερεις διαφορετικές καταστάσεις (modes) [E314]:

- **Sniffer mode.** Σε αυτή την κατάσταση το Snort απλά διαβάζει τα πακέτα εκτός δικτύου και τα εμφανίζει σαν μια συνεχόμενη ροή στην οθόνη.

- **Packet Logger mode.** Καταγράφει τα δεδομένα στο δίσκο.
- **Network Intrusion Detection System mode.** Αυτή η κατάσταση έχει τις περισσότερες δυνατότητες και επιτρέπει στο Snort να αναλύει τη δικτυακή κίνηση πραγματοποιώντας μια σειρά από ενέργειες βασισμένες στα πακέτα που παρακολουθεί.
- **Inline mode.** Συλλέγει τα πακέτα από τα IP-tables αντί από το libpcap και με βάση ένα σύνολο κανόνων αποφασίζει ποια πακέτα θα απορριφτούν από τα IP-tables.

Το Snort πραγματοποιεί ανάλυση πρωτοκόλλων (protocol analysis), αναζητήσεις με πρότυπα και χρησιμοποιείται για την παθητική ανίχνευση ή το μπλοκάρισμα διαφόρων ειδών επιθέσεων, όπως η υπερχείλιση μνήμης (buffer overflow), η κρυφή σάρωση πορτών (stealth port scans) και οι προσπάθειες αναγνώρισης του λειτουργικού συστήματος (OS fingerprinting). Το Snort μπορεί να συνδυαστεί με άλλα εργαλεία, όπως τα sguil, OSSIM και το BASE για γραφική αναπαράσταση των δεδομένων της εισβολής.

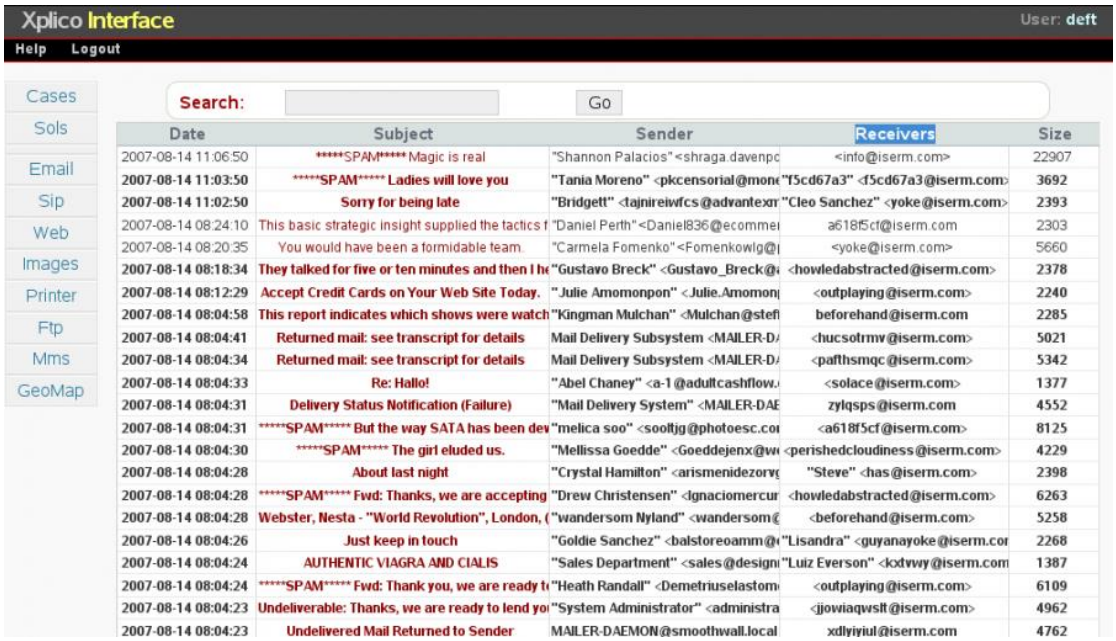
3.2.9 TCPflow

Το TCPflow είναι ένα εργαλείο (για χρήση σε περιβάλλον UNIX), το οποίο συλλέγει τα δεδομένα που μεταδίδονται ως μέρος των TCP συνδέσεων και τα αποθηκεύει. Σε αντίθεση με το Tcpdump, το οποίο παρουσιάζει μια περίληψη των πακέτων που παρακολουθεί και δεν αποθηκεύει τα δεδομένα που μεταδίδονται, το TCPflow ανακατασκευάζει τις ροές των δεδομένων και τις αποθηκεύει χωριστά σε αρχεία για περαιτέρω ανάλυση. Το TCPflow καταλαβαίνει τους αριθμούς ακολουθίας των πακέτων και μπορεί να ανακατασκευάσει τις ροές δεδομένων, ανεξάρτητα αν έχουν αναμεταδοθεί πακέτα. Ωστόσο, το TCPflow δεν καταλαβαίνει τις ροές που περιέχουν κατακερματισμένα πακέτα (IP fragments), δηλαδή πακέτα τα οποία έχουν κατακερματιστεί για να μπορέσουν να μεταδοθούν από κάποια σύνδεση με μικρότερο μέγεθος πακέτου (MTU) από το αρχικό. Βασίζεται στη βιβλιοθήκη συλλογής πακέτων LBL και υποστηρίζει την ίδια ποικιλία φίλτρων με το Tcpdump [E316].

3.2.10 Xplico

Το Xplico δεν είναι απλά ένας packet analyzer, είναι ένα NFAT (Network Forensics Analysis Tool) εργαλείο για UNIX. Το Xplico χρησιμοποιείται για την εξαγωγή δεδομένων που αφορούν τις εφαρμογές, από τη δικτυακή κίνηση που έχει συλλεχθεί. Για παράδειγμα μπορεί από ένα pcap αρχείο, να εξάγει όλα τα e-mail που μεταφέρθηκαν με τα πρωτόκολλα POP, IMAP και SMTP, καθώς και τα περιεχόμενα τα οποία μεταφέρθηκαν με το πρωτόκολλο HTTP, FTP, TFTP και VoIP. [E317]

Το Xplico μπορεί να χρησιμοποιηθεί και από την κονσόλα UNIX συστημάτων αλλά και μέσα από γραφικό περιβάλλον, μέσω του Web interface. Στην εικόνα 3.4 φαίνεται μια λίστα με όλα τα e-mails που στάλθηκαν και λήφθηκαν μαζί με κάποιες πληροφορίες, όπως η ημερομηνία και η ώρα αποστολής, το θέμα του μηνύματος, το όνομα του αποστολέα και του παραλήπτη (ακόμα και αν χρησιμοποιήθηκε κρυφή κοινοποίηση) και το μέγεθος του e-mail.

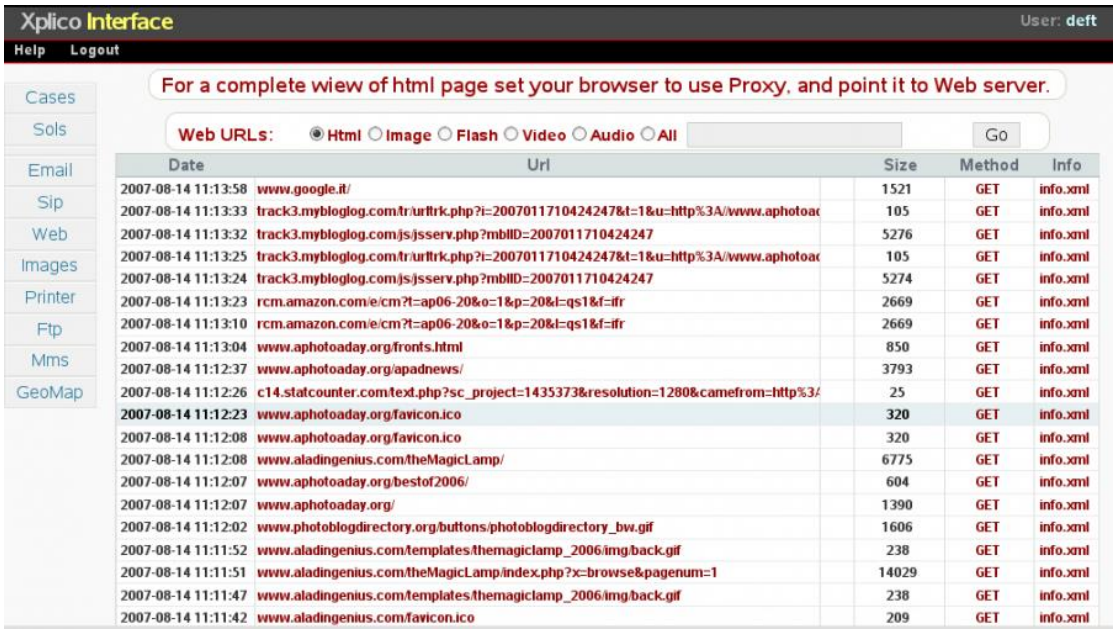


Εικόνα 3.4. Στιγμιότυπο του Xplico

Μέσω του πεδίου αναζήτησης, υπάρχει η δυνατότητα αναζήτησης e-mail, με βάση κάποιου από τα χαρακτηριστικά που αναφέρθηκαν.

Στην εικόνα 3.5 φαίνονται τα περιεχόμενα μιας HTTP συνόδου. Επιλέγοντας κάποιο από τα περιεχόμενα, το Xplico θα αναδημιουργήσει το πλήρες URL της

σελίδας. Επίσης, μπορεί να προσομοιώσει την μνήμη cache του φυλλομετρητή (browser), εφόσον αυτά τα δεδομένα περιέχονται στο pcap αρχείο. Πέρα από αυτά, υπάρχει η δυνατότητα να εξεταστούν οι κεφαλίδες της αίτησης (request) και της απόκρισης (response).



Εικόνα 3.5. Στιγμιότυπο που απεικονίζει περιεχόμενα μιας HTTP συνόδου

3.2.11 NetworkMiner

Το NetworkMiner είναι ένα NFAT εργαλείο για Windows. Χρησιμοποιείται ως network sniffer/packet sniffer για να ανιχνεύσει λειτουργικά συστήματα, συνόδους (sessions), ονόματα υπολογιστών (hostnames), ανοιχτές πόρτες και άλλα. Το NetworkMiner έχει παθητική λειτουργία , δηλαδή απλά συλλέγει δεδομένα χωρίς όμως να αποστέλλει καθόλου πακέτα προς το δίκτυο, κάνοντας σχεδόν αδύνατη την ανίχνευση της ύπαρξης του. Μπορεί να πραγματοποιήσει ανάλυση PCAP αρχείων και να ανασυναρμολογήσει τα δεδομένα. Ο κυριότερος σκοπός του είναι να συλλέγει δεδομένα για τους υπολογιστές του δικτύου παρά να συλλέγει την κίνηση του δικτύου. Το NetworkMiner μπορεί να συλλέξει στοιχεία για τα λειτουργικά συστήματα (OS fingerprinting) βασιζόμενο στα πακέτα TCP SYN και SYN+ACK. [E318]

ΚΕΦΑΛΑΙΟ 4

Η Εφαρμογή PacketViewer

Για τις ανάγκες της παρούσας πτυχιακής εργασίας αναπτύχθηκε η εφαρμογή PacketViewer, με σκοπό την καλύτερη παρουσίαση των βασικών πληροφοριών που περιέχονται στα πακέτα που λαμβάνονται και ανταλλάσσονται σε ένα δίκτυο υπολογιστών. Σε αυτή την ενότητα γίνεται περιγραφή του τεχνολογικού περιβάλλοντος υλοποίησης της εφαρμογής καθώς επίσης και της λειτουργίας-χρήσης της.

4.1 Τεχνολογικό περιβάλλον υλοποίησης

Η εφαρμογή PacketViewer αποτελεί ένα βοηθητικό εργαλείο, το οποίο λειτουργεί σε συνεργασία με το WireShark και αποσκοπεί στην καλύτερη παρουσίαση και επομένως εποπτεία των πακέτων που έχουν συλλεχθεί, τα οποία περιέχουν δικτυακά δεδομένα και προορίζονται για περαιτέρω εξέταση. Καταρχήν, για την σύλληψη των πακέτων χρησιμοποιήθηκε το WireShark, το οποίο αποτελεί ίσως το γνωστότερο network protocol analyzer εργαλείο. Μια λεπτομερέστερη περιγραφή του WireShark γίνεται στην ενότητα 3.2.2 όπου επίσης περιγράφεται η διαδικασία συλλογής δεδομένων από ένα δίκτυο. Αφού συλλεχθεί ο επιθυμητός αριθμός πακέτων, γίνεται εξαγωγή αυτών σε ένα XML αρχείο, δυνατότητα που υποστηρίζεται από το WireShark (File > Export).

Η εφαρμογή PacketViewer, σχεδιάστηκε ώστε να δέχεται τέτοιας μορφής xml αρχεία από το WireShark, τα οποία χρησιμοποιεί για να αντλήσει τις πληροφορίες που χρειάζεται και να τις εισάγει στο πρόγραμμα. Για την υλοποίηση της εφαρμογής χρησιμοποιήθηκε η γλώσσα προγραμματισμού Java (έκδοση jdk1.6.0_13). Για την επεξεργασία των XML αρχείων χρησιμοποιήθηκε το μοντέλο JDOM (Java Document Object Model). Το JDOM παρέχει τον τρόπο πρόσβασης στα στοιχεία του XML αρχείου, μέσω μιας δενδρικής δομής (όπως και το DOM). Το JDOM απαρτίζεται από δέκα κλάσεις, οι οποίες αναπαριστούν τα διαφορετικά

στοιχεία του XML εγγράφου και με τις μεθόδους των οποίων μπορεί να γίνει η επεξεργασία της δομής, που δημιουργείται σαν αναπαράσταση του XML. Ένα αντικείμενο Document είναι η αναπαράσταση όλου του XML εγγράφου και συγχρόνως περιέχει όλα τα άλλα JDOM αντικείμενα. Για την εισαγωγή του XML εγγράφου το JDOM βασίζεται στον SAX parser, δημιουργώντας έναν SAXBuilder, ο οποίος μετατρέπει το XML έγγραφο σε ένα document δίνοντας τη δυνατότητα αναδρομικής διέλευσης όλων των στοιχείων.

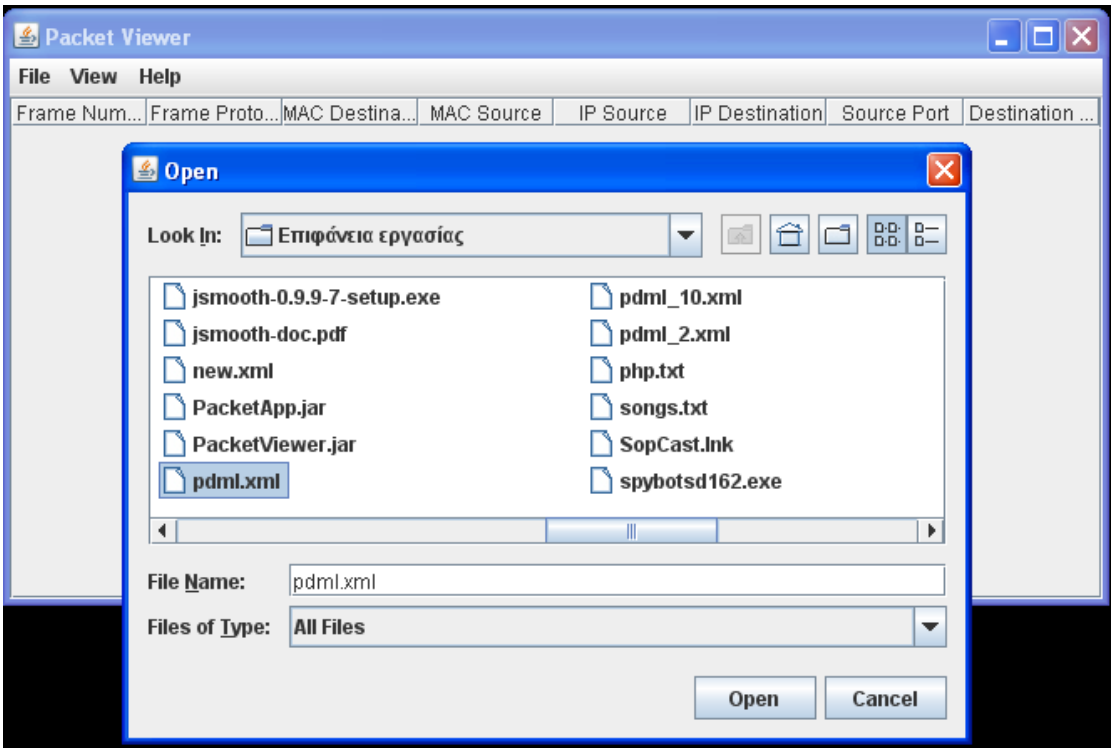
Τα δεδομένα που έχουν επιλεχθεί από το XML έγγραφο, εισάγονται σε μια βάση δεδομένων MS-Access ώστε να γίνει ευκολότερη η διαχείριση τους. Η βάση, η οποία αρχικά είναι κενή μέχρις ότου εισαχθεί ένα XML αρχείο, περιλαμβάνει τα εξής πεδία:

- Frame Number
- Frame Protocols
- MAC Destination
- MAC Source
- IP Source
- IP Destination
- TCP/UDP Source Port
- TCP/UDP Destination Port

Μετά την εισαγωγή του XML αρχείου και την φόρτωση των δεδομένων στη βάση, η εφαρμογή επικοινωνεί μόνο με τη βάση κάθε φορά που ο χρήστης επιθυμεί να αλλάξει τη διάταξη των δεδομένων ταξινομώντας τα με βάση κάποιο από τα παραπάνω πεδία.

4.2 Περιγραφή λειτουργίας της εφαρμογής

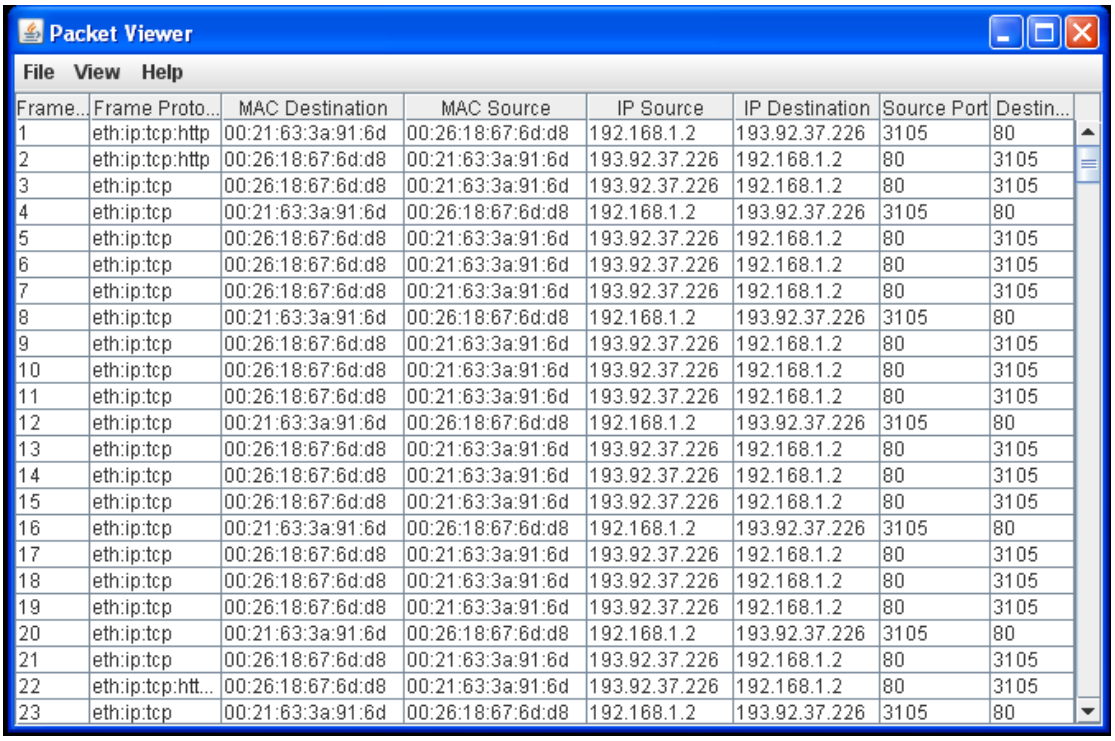
Όπως αναφέρθηκε προηγουμένως, για τη λειτουργία της εφαρμογής προαπαιτείται η ύπαρξη ενός XML αρχείου με δικτυακά δεδομένα, το οποίο θα αποτελέσει την είσοδο στην εφαρμογή.



Εικόνα 4.1. Στιγμιότυπο της εφαρμογής PacketViewer κατά το άνοιγμα αρχείου

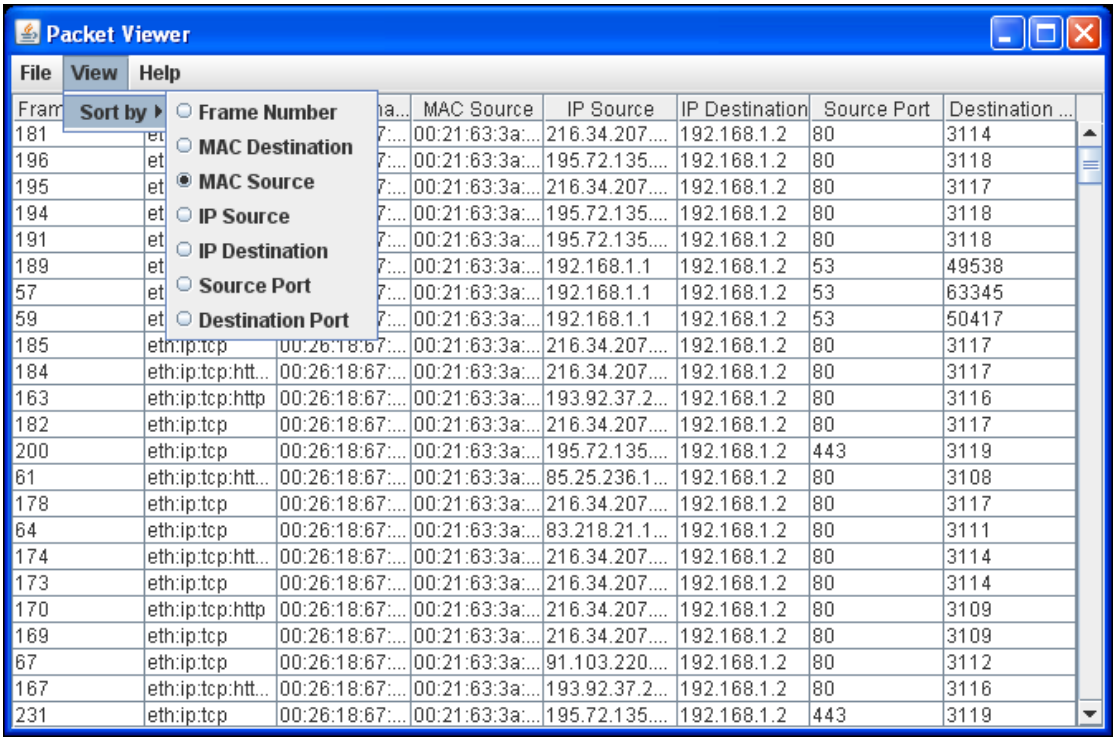
Η είσοδος ενός XML αρχείου γίνεται πολύ εύκολα επιλέγοντας από το μενού “File” την επιλογή “Open file” και στη συνέχεια από το παράθυρο που εμφανίζεται, γίνεται η πλοήγηση στους καταλόγους για τον προσδιορισμό του επιθυμητού XML αρχείου, όπως φαίνεται στην εικόνα 4.1.

Αφού γίνει η επιλογή του αρχείου, εμφανίζονται τα δεδομένα (εικόνα 4.2) στα αντίστοιχα πεδία του πίνακα ταξινομημένα με βάση τον αριθμό πλαισίου (Frame Number). Εάν το ενδιαφέρον επικεντρώνεται σε κάποιο άλλο χαρακτηριστικό των δεδομένων, όπως για παράδειγμα η διεύθυνση IP προέλευσης των πακέτων, τότε από το μενού “View” και το υπομενού “Sort by”, επιλέγοντας το επιθυμητό πεδίο ταξινόμησης των δεδομένων, γίνεται η αντίστοιχη ταξινόμηση των δεδομένων σε αύξουσα σειρά (εικόνα 4.3).



Frame...	Frame Proto...	MAC Destination	MAC Source	IP Source	IP Destination	Source Port	Destin...
1	eth:ip:tcp:http	00:21:63:3a:91:6d	00:26:18:67:6d:d8	192.168.1.2	193.92.37.226	3105	80
2	eth:ip:tcp:http	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
3	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
4	eth:ip:tcp	00:21:63:3a:91:6d	00:26:18:67:6d:d8	192.168.1.2	193.92.37.226	3105	80
5	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
6	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
7	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
8	eth:ip:tcp	00:21:63:3a:91:6d	00:26:18:67:6d:d8	192.168.1.2	193.92.37.226	3105	80
9	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
10	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
11	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
12	eth:ip:tcp	00:21:63:3a:91:6d	00:26:18:67:6d:d8	192.168.1.2	193.92.37.226	3105	80
13	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
14	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
15	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
16	eth:ip:tcp	00:21:63:3a:91:6d	00:26:18:67:6d:d8	192.168.1.2	193.92.37.226	3105	80
17	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
18	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
19	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
20	eth:ip:tcp	00:21:63:3a:91:6d	00:26:18:67:6d:d8	192.168.1.2	193.92.37.226	3105	80
21	eth:ip:tcp	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
22	eth:ip:tcp:htt...	00:26:18:67:6d:d8	00:21:63:3a:91:6d	193.92.37.226	192.168.1.2	80	3105
23	eth:ip:tcp	00:21:63:3a:91:6d	00:26:18:67:6d:d8	192.168.1.2	193.92.37.226	3105	80

Εικόνα 4.2. Στιγμιότυπο του πίνακα δεδομένων της εφαρμογής PacketViewer



Fram...			MAC Source	IP Source	IP Destination	Source Port	Destination ...
181	et	7:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3114
196	et	7:...	00:21:63:3a:...	195.72.135....	192.168.1.2	80	3118
195	et	7:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3117
194	et	7:...	00:21:63:3a:...	195.72.135....	192.168.1.2	80	3118
191	et	7:...	00:21:63:3a:...	195.72.135....	192.168.1.2	80	3118
189	et	7:...	00:21:63:3a:...	192.168.1.1	192.168.1.2	53	49538
57	et	7:...	00:21:63:3a:...	192.168.1.1	192.168.1.2	53	63345
59	et	7:...	00:21:63:3a:...	192.168.1.1	192.168.1.2	53	50417
185	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3117
184	eth:ip:tcp:htt...	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3117
163	eth:ip:tcp:http	00:26:18:67:...	00:21:63:3a:...	193.92.37.2...	192.168.1.2	80	3116
182	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3117
200	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	195.72.135....	192.168.1.2	443	3119
61	eth:ip:tcp:htt...	00:26:18:67:...	00:21:63:3a:...	85.25.236.1...	192.168.1.2	80	3108
178	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3117
64	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	83.218.21.1...	192.168.1.2	80	3111
174	eth:ip:tcp:htt...	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3114
173	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3114
170	eth:ip:tcp:http	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3109
169	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	216.34.207....	192.168.1.2	80	3109
67	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	91.103.220....	192.168.1.2	80	3112
167	eth:ip:tcp:htt...	00:26:18:67:...	00:21:63:3a:...	193.92.37.2...	192.168.1.2	80	3116
231	eth:ip:tcp	00:26:18:67:...	00:21:63:3a:...	195.72.135....	192.168.1.2	443	3119

Εικόνα 4.3. Στιγμιότυπο της εφαρμογής PacketViewer κατά την επιλογή πεδίου ταξινόμησης

ΚΕΦΑΛΑΙΟ 5

Αιχμή της τεχνολογίας στη δικανική δικτύων

Wireless Forensics

5.1 Εισαγωγή

Η ευρεία αποδοχή και χρήση των ασύρματων τεχνολογιών τα τελευταία χρόνια, έχει φέρει στο επίκεντρο τα ασύρματα δίκτυα δεδομένων (Wi-Fi), που βασίζονται στις προδιαγραφές του 802.11 της IEEE. Ωστόσο, η ασύρματη φύση της νέας τεχνολογίας, έχει προκαλέσει ανησυχίες στους υπεύθυνους ασφαλείας και στους διαχειριστές δικτύων, καθώς παρατηρείται ολοένα και μεγαλύτερος αριθμός επιθέσεων μέσω ασύρματων δικτύων. Λόγω της νεότητας της τεχνολογίας, υπάρχουν μεγαλύτερα κενά στην ασφάλεια των ασύρματων δικτύων, σε σχέση με τα αντίστοιχα ενσύρματα δίκτυα, πράγμα που εκμεταλλεύονται οι φιλόδοξοι και κακόβουλοι εισβολείς.

Στην παρούσα ενότητα παρουσιάζονται τα ζητήματα που σχετίζονται με τη συλλογή και την ανάλυση της δικτυακής κίνησης, από ασύρματα δίκτυα. Δίνεται έμφαση στις τεχνικές δυσκολίες και στις προκλήσεις που παρουσιάζει η συλλογή της δικτυακής κίνησης στα ασύρματα δίκτυα, καθώς επίσης προτείνονται κάποιες τεχνικές και μέθοδοι για την καλύτερη σχεδίαση εργαλείων ασύρματης δικανικής (wireless forensics tools). Τέλος, παρουσιάζονται οι κυριότερες προκλήσεις κατά την ανάλυση της δικτυακής κίνησης και κάποιες τεχνικές αντι-δικανικής (anti-forensics), τις οποίες χρησιμοποιούν οι επιτιθέμενοι για να καλύπτουν τα ίχνη τους.

Κύριος σκοπός της ασύρματης δικανικής δικτύων, είναι να παράσχει τη μεθοδολογία και τα εργαλεία που απαιτούνται, για τη συλλογή και την ανάλυση της δικτυακής κίνησης με έγκυρο τρόπο, ώστε τα ψηφιακά αποδεικτικά στοιχεία να μπορέσουν να παρουσιαστούν σε κάποιο δικαστήριο [E41]. Η ασύρματη δικανική διαδικασία περιλαμβάνει τη συλλογή όλων των δεδομένων που μεταδίδονται στο δίκτυο και την ανάλυση τους, ώστε να αποκαλυφθούν ανωμαλίες του δικτύου και

να ανακαλυφθούν οι πηγές των επιθέσεων. Γενικά, ισχύουν οι ίδιες αρχές που εφαρμόζονται στην δικανική υπολογιστών (computer forensics): συλλογή, εξέταση, ανάλυση και αναφορά των αποτελεσμάτων.

5.2 Τεχνικές προκλήσεις κατά την ασύρματη σύλληψη δεδομένων

Το βασικότερο πρόβλημα που παρουσιάζεται στην ασύρματη δικανική, έγκειται στην ίδια τη φύση των ραδιοσυχνοτήτων και στην πολυπλοκότητα που εισάγουν οι προδιαγραφές του 802.11. Τα ασύρματα δίκτυα 802.11, χωρίζουν το φάσμα συχνοτήτων σε διάφορα κανάλια, όπως φαίνεται στην εικόνα 4.1, τα οποία χρησιμοποιούνται για την επίτευξη μη επικαλυπτόμενων επικοινωνιών.

Ένα εργαλείο ασύρματης δικανικής, θα πρέπει να διαθέτει ασύρματη κάρτα, η οποία να υποστηρίζει πολλαπλές διαμορφώσεις (όπως το Atheros). Τα συνήθη εργαλεία διαθέτουν μόνο μια ασύρματη κάρτα και έτσι μπορούν να παρακολουθούν ένα συγκεκριμένο κανάλι κάθε στιγμή. Αυτά τα εργαλεία χρησιμοποιούν την τεχνική αναπήδησης καναλιών (channel hoping), ώστε να παρακολουθούν όλο το φάσμα συχνοτήτων, παίρνοντας όμως ένα μικρό δείγμα από κάθε κανάλι.

Έκδοση 802.11	Εύρος καναλιού	Ακτίνα συχνοτήτων	Τύπος φάσματος	Ρυθμός μετάδοσης
802.11a	20 MHz	5160-5330 MHz	OFDM	54 Mbps
802.11b	22 MHz	2401-2495 MHz	DSSS	11 Mbps
802.11g	22/20 MHz	2401-2495 MHz	DSSS/OFDM	54 Mbps

Εικόνα 5.1. Προδιαγραφές του 802.11

Όταν υπάρχει μόνο ένα ασύρματο σημείο πρόσβασης (access point), δεν υπάρχει πρόβλημα για τη σύλληψη των δεδομένων, καθώς το σημείο πρόσβασης εκπέμπει σε ένα μόνο κανάλι. Πλέον, η ύπαρξη πολλαπλών ασύρματων σημείων πρόσβασης είναι συνηθισμένη, για αυτό ένα εργαλείο ασύρματης δικανικής (wireless forensics tool), θα πρέπει να είναι ικανό να συλλέγει ταυτόχρονα τη δικτυακή κίνηση από όλα τα ασύρματα δίκτυα που υπάρχουν σε μια περιοχή, όπου θεωρείται ότι βρίσκεται ο επιτιθέμενος. Παρόλο που η νομοθεσία και οι

προδιαγραφές του 802.11 καθορίζουν ποια κανάλια θα χρησιμοποιούνται ανά χώρα, οι επιτιθέμενοι (όπως συνηθίζεται), δεν ακολουθούν τη νομοθεσία και επομένως είναι αναγκαία η παρακολούθηση και η σύλληψη δεδομένων και από τα 14 διαθέσιμα κανάλια.

Ένα από τα βασικά πλεονεκτήματα των ασύρματων δικτύων, είναι η δυνατότητα κίνησης και περιήγησης που παρέχουν στους χρήστες. Η δυνατότητα δηλαδή, ο χρήστης να μετακινείται στην περιοχή του ασύρματου δικτύου χωρίς να χάνεται η σύνδεση. Αυτό επιτυγχάνεται με την γρήγορη εναλλαγή σημείων πρόσβασης. Μόλις η κάρτα δικτύου εντοπίσει αδύναμο σήμα στο τρέχων σημείο πρόσβασης, αλλάζει κανάλι ώστε να βρει δυνατότερο σήμα. Αν το εργαλείο που συλλέγει τα πακέτα, δεν καταγράφει όλα τα κανάλια, τότε μέρος των δεδομένων δεν θα καταγραφεί. Αυτό το πλεονέκτημα των ασύρματων δικτύων, γίνεται πρόκληση στην ασύρματη δικανική.

Για την σύλληψη της ασύρματης δικτυακής κίνησης, υπάρχουν κάποια επιπλέον χαρακτηριστικά που θα πρέπει να ληφθούν υπ’ όψιν, όπως ο τύπος των πλαισίων (frames), το μέγεθος τους, ο αριθμός των πλαισίων (κατά προσέγγιση) καθώς και τις απαιτήσεις σε εύρος ζώνης (bandwidth). Το μέγιστο μέγεθος του μεταδιδόμενου πλαισίου (MTU – Maximum Transmission Unit), όταν αυτό μεταφέρει δεδομένα, ορίζεται από τις προδιαγραφές του 802.11 στα 2304 bytes [E43]. Το μέγεθος αυτό δεν περιλαμβάνει το επιπλέον φορτίο που προστίθεται από τη χρήση κρυπτογράφησης, το οποίο ποικίλει ανάλογα με τη μέθοδο (για WEP απαιτούνται 8 επιπλέον bytes, για WPA 20 επιπλέον bytes και για WPA2 16 επιπλέον bytes). Σε κάθε περίπτωση, το μέγεθος του MTU είναι κατά πολύ μεγαλύτερο από το αντίστοιχο του Ethernet που αντιστοιχεί στα 1500 bytes.

Επιπρόσθετα, οι προδιαγραφές του 802.11 ορίζουν τρείς τύπους πλαισίων, που απαιτούνται για τη διαχείριση της αναξιοπιστίας, που εισάγει το μέσο μετάδοσης (ραδιοσυχνότητες): τα πλαίσια ελέγχου, τα πλαίσια διαχείρισης και τα πλαίσια δεδομένων. Οι δυο πρώτοι τύποι υπάρχουν μόνο στα ασύρματα δίκτυα και επηρεάζουν τη συνολική ποσότητα δεδομένων που συλλέγεται. Από την πλευρά της σχεδίασης του υλικού, η ασύρματη συσκευή συλλογής πακέτων, θα πρέπει να μπορεί να ανταπεξέλθει στη μέγιστη θεωρητική διεκπεραιωτική ικανότητα που αφορά και τα 14 κανάλια επικοινωνίας.

5.3 Εργαλεία υποστήριξης της ασύρματης δικανικής

Μερικά από τα εργαλεία που κυκλοφορούν και μπορούν να χρησιμοποιηθούν για ασύρματη δικανική είναι τα εξής:

- Το Janus Project [E45] είναι ένα εμπορικό εργαλείο το οποίο παρουσιάστηκε το 2006 και περιέχει 8 ασύρματες κάρτες δικτύου για ασύρματη σάρωση (scanning), σύλληψη δεδομένων και δυνατότητες αποκρυπτογράφησης.

- Το WLAN-14 [E46] είναι μια εμπορική συσκευή για χρήση σε Linux συστήματα και σχεδιάστηκε για την ασφαλή σύλληψη δεδομένων σε ασύρματα δίκτυα 802.11 b/g. Διαθέτει 15 ασύρματες κάρτες, GPS, υποδοχή εξωτερικής κεραίας και δυνατότητα εναλλαγής δίσκων (hot-swappable disks).

- Το AirCapture [E44] είναι ένα εμπορικό εργαλείο με δυνατότητες ταυτόχρονης σύλληψης όλων των δεδομένων που μεταδίδονται και αποθήκευσης τους για ανάλυση. Είναι πλήρως παθητικό και διαθέτει GPS με το οποίο εντοπίζεται η ακριβής τοποθεσία από όπου έγινε η συλλογή των στοιχείων-δεδομένων.

5.4 Προτάσεις και τεχνικές για τη σχεδίαση εργαλείων ασύρματης δικανικής

Τα περισσότερα εργαλεία που έχουν κυκλοφορήσει μέχρι σήμερα λειτουργούν κυρίως ως εργαλεία cracking και δεν διαθέτουν τις απαιτούμενες λειτουργίες για να χρησιμοποιηθούν για το σκοπό της ασύρματης δικανικής. Παρακάτω παρουσιάζονται οι προτεινόμενες και επιθυμητές λειτουργίες που θα πρέπει να έχουν τα εργαλεία που προορίζονται για την ασύρματη δικανική.

- Μια συσκευή, για να μπορεί να παρακολουθεί και τα 14 κανάλια του 802.11 θα πρέπει να διαθέτει 15 ασύρματες κάρτες δικτύου. Η 15η κάρτα

χρησιμοποιείται για να ελέγχει συνεχώς τα κανάλια σε όλο το φάσμα για να εντοπίσει τυχόν νέα ασύρματα δίκτυα.

- Η χρήση GPS είναι απαραίτητη, καθώς μπορεί να δώσει ακριβείς πληροφορίες χρονοσφραγίδας (timestamp) και τοποθεσίας, για το που και το πότε έγινε η σύλληψη των δεδομένων.
- Κατά την σύλληψη των δικτυακών δεδομένων δεν θα πρέπει να εφαρμόζεται κανένα φίλτρο εκτός και αν επιβάλλεται για κάποιο λόγο.

- Γενικά, όλα τα εργαλεία που χρησιμοποιούνται στη δικανική (είτε ασύρματη είτε ενσύρματη) θα πρέπει να έχουν πλήρως παθητική λειτουργία και να μην εισάγουν καθόλου κίνηση στο δίκτυο.

- Η συσκευή θα πρέπει να διαθέτει θύρα σύνδεσης εξωτερικής κεραίας ώστε να μπορεί να επεκτείνει τις δυνατότητες λήψης, σε μεγαλύτερη εμβέλεια.

- Η συλλογή των δεδομένων θα πρέπει να γίνεται στην τυποποιημένη PCAP μορφή, ώστε να είναι αναγνωρίσιμη από τα περισσότερα εμπορικά και ανοιχτού κώδικα εργαλεία.

- Το υλικό από το οποίο θα απαρτίζεται η συσκευή, θα πρέπει να έχει μεγάλη ευαισθησία στη λήψη, ώστε να αυξάνονται οι πιθανότητες συλλογής της δικτυακής κίνησης ακόμα και κάτω από κακές συνθήκες.

5.5 Τεχνικές προκλήσεις κατά την Ανάλυση της ασύρματης δικτυακής κίνησης

Για την ανάλυση της ασύρματης δικτυακής κίνησης απαιτούνται οι ίδιες δυνατότητες όπως και στην ενσύρματη δικανική δικτύων, δηλαδή γνώση των πρωτοκόλλων που εμπλέκονται στη μετάδοση των δεδομένων. Πιο συγκεκριμένα, στα ασύρματα αυτό σημαίνει, τα πρωτόκολλα που βασίζονται στο TCP/IP και χρησιμοποιούνται στο 802.11. Το NetIntercept και το eTrust NF είναι δυο ολοκληρωμένα εμπορικά εργαλεία με δυνατότητες ανάλυσης και εξειδικευμένες

λειτουργίες χειρισμού των κεφαλίδων του 802.11. Τα μη εμπορικά εργαλεία ανοιχτού κώδικα που παρουσιάστηκαν σε προηγούμενο κεφάλαιο (Wireshark, Tcpdump κλπ) μπορούν επίσης να χρησιμοποιηθούν στην ανάλυση των δεδομένων της ασύρματης δικανικής. Η διαδικασία της ανάλυσης είναι παρόμοια και στις δύο περιπτώσεις, για αυτό το ενδιαφέρον επικεντρώνεται σε συγκεκριμένα τεχνικά θέματα που αφορούν το στάδιο της ανάλυσης, της ασύρματης κίνησης δεδομένων.

Ένα από τα πρώτα ζητήματα που θα πρέπει να αντιμετωπιστούν, είναι η συγχώνευση των PCAP αρχείων (που περιέχουν τα δεδομένα που συλλέχθηκαν) και τα οποία αντιστοιχούν σε όλα τα κανάλια. Σε ένα εργαλείο με πολλές ασύρματες κάρτες, η κάθε κάρτα παρακολουθεί ένα συγκεκριμένο κανάλι και συγκεντρώνει τα δεδομένα σε ένα PCAP αρχείο. Στην περίπτωση ενός χρήστη του δικτύου, ο οποίος περιηγείται μέσα σε αυτό, απαιτείται η συγχώνευση των δεδομένων από τα διάφορα κανάλια ώστε να ξαναδημιουργηθεί η σύνοδος. Για τη συγχώνευση μπορεί να χρησιμοποιηθεί το εργαλείο mergecap που περιέχεται στο Wireshark και δίνει τη δυνατότητα συγχώνευσης πολλαπλών PCAP αρχείων σε ένα.

Δεύτερον, ένα PCAP αρχείο (και γενικά ένα αρχείο που περιέχει συλλεγμένα δεδομένα) από ένα συγκεκριμένο κανάλι, μπορεί να περιέχει δεδομένα από επικαλυπτόμενα κανάλια, δηλαδή από άλλα δίκτυα σε γειτονικά κανάλια. Οι πιθανότητες να συμβεί κάτι τέτοιο, εξαρτώνται από την ισχύ της εκπομπής του σημείου πρόσβασης (access point), την ευαισθησία της συσκευής λήψης και την κεραία που χρησιμοποιείται. Κατά τη διάρκεια του σταδίου της ανάλυσης, είναι απαραίτητο να αναγνωριστούν και να απορριφθούν τα διπλά πλαίσια.

Τέλος, το πιο χρήσιμο χαρακτηριστικό όταν υπάρχει μεγάλος όγκος δεδομένων προς διαχείριση, είναι η δυνατότητα φιλτραρίσματος. Μετά την συγχώνευση της κίνησης του δικτύου σε ένα PCAP αρχείο, με τη χρήση φίλτρων είναι δυνατή η εμφάνιση της κίνησης που σχετίζεται με ένα χρήστη του δικτύου σε όλα τα κανάλια, βασισμένο στη MAC διεύθυνση του. Εναλλακτικά μπορεί να χρησιμοποιηθεί φίλτρο βασισμένο στο BSSID (Basic Service Set Identifier), για την εμφάνιση της κίνησης σε ένα συγκεκριμένο σημείο πρόσβασης.

5.6 Ασύρματη κρυπτογράφηση

Οι προδιαγραφές του 802.11 ενσωματώνουν διάφορους τύπους κρυπτογράφησης (2ου επιπέδου) των δεδομένων. Το βασικό πρόβλημα που πρέπει να αντιμετωπιστεί, είναι η απόκτηση-εύρεση του κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση της ασύρματης κίνησης των δεδομένων. Χωρίς το κλειδί δεν μπορεί να γίνει η ανάλυση των δεδομένων και επομένως η εύρεση του είναι επιτακτική για την όλη δικανική διαδικασία. Στον παρακάτω πίνακα φαίνονται οι τύποι κρυπτογράφησης και τα εργαλεία με τα οποία μπορούν να παρακαμφθούν.

Κρυπτογράφηση	Κλειδί	Επίπεδο ασφαλείας	Εργαλείο αντιμετώπισης	Εύρεση κλειδιού
Ανοιχτή	Όχι	N/A	Sniffer	Δεν απαιτείται
WEP	PSK	Χαμηλό	Aircrack -ng	Εφικτή
WPA WPA2-Personal	PSK	Μεσαίο	CoWPAtty	Εφικτή
WPA WPA2-Enterprise	EAP	Υψηλό	N/A	Άλλοι τρόποι

Εικόνα 5.2. Τύποι κρυπτογράφησης

Με την σύλληψη αρκετών δεδομένων από το ασύρματο δίκτυο, είναι πάντα εφικτό να βρεθεί το κλειδί, όταν χρησιμοποιείται κρυπτογράφηση WEP και των παράγωγων τεχνικών (WEP+, DWEP κλπ.). Το WEP θεωρείται μη ασφαλής μηχανισμός κρυπτογράφησης και μπορεί εύκολα και με πολλούς τρόπους να παρακαμφθεί. Το WPA/PSK στηρίζει το επίπεδο ασφαλείας του στο κλειδί του (pre-shared key). Αν το κλειδί είναι αρκετά μεγάλο και δεν βασίζεται σε έτοιμες λέξεις που υπάρχουν σε λεξικά ή να μπορούν να παραχθούν από αυτά, τότε το επίπεδο ασφαλείας του είναι αρκετά μεγάλο. Σε αντίθετη περίπτωση το κλειδί μπορεί να ανακαλυφθεί σχετικά εύκολα με την τεχνική της επίθεσης λεξικού (dictionary attack) ή με τη χρήση προϋπολογισμένων κλειδιών. Στο WPA2/Enterprise, το κλειδί κρυπτογράφησης παράγεται τυχαία από τον RADIUS server και έτσι η επίθεση λεξικού δεν έχει μεγάλη χρησιμότητα σε αυτή την περίπτωση. Η αδυναμία της μεθόδου βρίσκεται στο μηχανισμό αυθεντικοποίησης των μεθόδων που παρέχει το EAP (Extensible Authentication Protocol). Γενικά μόνο η κρυπτογράφηση με WPA και WPA2/ Personal με ισχυρό κλειδί (PSK) τουλάχιστον 20 χαρακτήρων (όπως ορίζει η προδιαγραφή IEEE 802.11i) μπορεί να θεωρηθεί ισχυρή, καθώς και η WPA2/Enterprise με δυνατά EAP πρωτόκολλα

(PEAP, EAP/TLS). Σε αυτές τις περιπτώσεις απαιτούνται άλλοι τρόποι ώστε να μπορέσει ο αναλυτής να αποκτήσει πρόσβαση στα δεδομένα.

Επίσης, αρκετά συχνή είναι και η χρήση κρυπτογράφησης σε ανώτερα επίπεδα από αυτό του 2ου, όπως στα VPN χρησιμοποιώντας IPSec, SSL ή SSH. Φυσικά αυτού του είδους η κρυπτογράφηση σε ανώτερα πρωτόκολλα, δεν εφαρμόζεται μόνο στα ασύρματα δίκτυα αλλά μπορεί να χρησιμοποιηθεί και στα ενσύρματα. Σε κάθε περίπτωση, αν ο επιτιθέμενος χρησιμοποιήσει κάποιο τρίτο ασύρματο δίκτυο για να πετύχει τους σκοπούς του, αυτό σημαίνει ότι θα αντιμετωπίσει τις ίδιες δυσκολίες και τους περιορισμούς που εισάγει η κρυπτογράφηση, όπως και ο αναλυτής. Επομένως αν ο επιτιθέμενος κατάφερε να ξεπεράσει με επιτυχία το εμπόδιο της κρυπτογράφησης, αυτό σημαίνει ότι χρησιμοποίησε κάποιο ανοικτό δίκτυο (χωρίς ασφάλεια) ή ότι η μέθοδος κρυπτογράφησης δεν ήταν αρκετά ασφαλής (WEP) ή ότι το κλειδί ήταν εύκολο να βρεθεί.

Αν η κρυπτογράφηση 2ου επιπέδου δε μπορεί να παρακαμφθεί, αυτομάτως δε μπορούν να εξαχθούν περισσότερες από τα περιεχόμενα. Βέβαια τα πλαίσια διαχείρισης και ελέγχου είναι πάντα διαθέσιμα, καθώς μεταφέρονται πάντα υπό μορφή καθαρού κειμένου και είναι ικανά να δώσουν από μόνα τους κάποιες πληροφορίες, όπως αν επιτεύχθηκε μια σύνδεση ή όχι και τη μέθοδο αυθεντικοποίησης που χρησιμοποιήθηκε.

5.7 Τεχνικές ασύρματης αντι-δικανικής

Υπάρχουν διάφορες τεχνικές και εργαλεία, τα οποία χρησιμοποιούνται από τους επιτιθέμενους και έχουν ως σκοπό την παρεμπόδιση της δικανικής διαδικασίας. Καθώς οι τεχνικές της ασύρματης δικανικής θα εξελίσσονται, νέες μέθοδοι ασύρματης αντι-δικανικής θα εμφανίζονται και θα χρησιμοποιούνται από τους επιτιθέμενους. Στην παρούσα παράγραφο παρουσιάζονται κάποιες πληροφορίες για μεθόδους αντι-δικανικής, οι οποίες θα προσφέρουν σημαντική βοήθεια στον δικανικό ερευνητή, ώστε να είναι ενήμερος στο τι μπορεί να αντιμετωπίσει.

Στην ασύρματη δικανική, τέτοιες μέθοδοι επιτυγχάνονται με τη χρήση παράνομων καναλιών (όπως για παράδειγμα η χρήση του καναλιού 14 στην Ευρώπη και στις ΗΠΑ) ή με τη χρήση ισχυρής κρυπτογράφησης 2ου επιπέδου. Ωστόσο υπάρχουν

και άλλες πιο εξελιγμένες τεχνικές, οι οποίες παρόλο που δεν σχεδιάστηκαν για αυτό το σκοπό, τελικά μπορούν να δώσουν πλεονέκτημα στον επιτιθέμενο, αν ο ερευνητής δεν είναι ενήμερος για αυτές. Δυο τέτοιες τεχνικές επιτυγχάνονται με τη χρήση κρυφών καναλιών (covert channels) και με την τροποποίηση των προδιαγραφών του 802.11.

Το “Raw Covert” [E47], είναι ένα εργαλείο το οποίο δημιουργεί κρυφά κανάλια μέσα σε 802.11 δίκτυα, χρησιμοποιώντας την τεχνική “raw injection”. Αυτή η τεχνική αποσκοπεί στην ενσωμάτωση πληροφοριών σε πλαίσια ελέγχου του 802.11. Πιο συγκεκριμένα, τα δεδομένα κωδικοποιούνται στο πεδίο της διεύθυνσης αποδέκτη (RA) των πλαισίων επιβεβαίωσης (ACK), δημιουργώντας έτσι ένα κρυφό κανάλι επικοινωνίας, το οποίο δεν μπορεί να ανιχνευτεί από τα εργαλεία ασύρματης παρακολούθησης, καθώς τα πλαίσια ACK συνήθως δεν εξετάζονται. Η μέθοδος μπορεί να εφαρμοστεί και σε άλλα πεδία των πλαισίων ελέγχου (CTS, RTS) ή των πλαισίων διαχείρισης ή ακόμα και σε μη έγκυρα πλαίσια.

Το “WiFi Advanced Stealth Patches” [E48, E49], είναι ένα σύνολο τροποποιήσεων για τον οδηγό “madwifi –ng” του Linux, που αφορά το chipset Atheros και το οποίο υλοποιεί ένα κρυφό, μη ανιχνεύσιμο πρωτόκολλο στο 2^{ο} επίπεδο του 802.11. Η τεχνική βασίζεται στην υλοποίηση μιας τροποποιημένης στοίβας δικτύου η οποία μπορεί να επικοινωνήσει μόνο με μια άλλη τροποποιημένη στοίβα. Με άλλα λόγια, ένα τροποποιημένο σημείο πρόσβασης μπορεί να επικοινωνήσει μόνο με ένα τροποποιημένο σύστημα κάποιου χρήστη. Αυτό το εργαλείο τροποποιεί το πεδίο πρωτοκόλλου του 802.11 και τον τύπο του πλαισίου. Με αυτό τον τρόπο, παρόλο που χρησιμοποιείται το καθορισμένο φάσμα συχνοτήτων, οι packet sniffers και τα IDS δεν μπορούν να αναγνωρίσουν την κίνηση.

ΚΕΦΑΛΑΙΟ 6

Συμπεράσματα – Μελλοντική Έρευνα

6.1 Προκλήσεις και κίνητρα στην ενσωμάτωση της δικανικής δικτύων

Η πλειοψηφία των δικλίδων ασφαλείας αποτυγχάνει να διαφυλάξει τα δίκτυα από παραβιάσεις και κακόβουλες ενέργειες. Παρά την αυξημένη χρήση IDS και firewall, παρατηρείται αύξηση των απειλών προς τα δίκτυα και παρουσιάζεται έλλειψη δυνατοτήτων διερεύνησης. Πολλές φορές οι επιθέσεις περνούν απαρατήρητες από τους μηχανισμούς ασφαλείας ή όταν ανιχνευτούν δεν υπάρχουν διαθέσιμα στοιχεία για αυτές. Υπάρχει επομένως ανάγκη για ενσωμάτωση δυνατοτήτων δικανικής στις υποδομές των δικτύων. Για να μπορέσει να γίνει αυτό, θα πρέπει πρώτα να ξεπεραστούν κάποιες τεχνικές και κοινωνικό-οικονομικές δυσκολίες [Sha03].

Τεχνικές δυσκολίες-προκλήσεις:

1. **Συλλογή δεδομένων.** Ένα δικανικό σύστημα θα πρέπει να παρακολουθεί και να συλλέγει ένα ευρύτερο φάσμα δεδομένων, καθώς δεν είναι εύκολο να προβλεφθεί τι στοιχεία μπορεί να χρειαστούν. Η συλλογή δεδομένων από τα σημεία εισόδου του δικτύου, δεν βοηθούν στην περίπτωση που υπάρξει κάποια εσωτερική επίθεση. Μια από τις μεγαλύτερες προκλήσεις στη δημιουργία ενός δικανικού συστήματος, είναι να παρακολουθεί και να συλλέγει ένα ευρύτερο φάσμα δεδομένων από πολλαπλές πηγές και πολλαπλά σημεία του δικτύου και να μπορεί να ανταπεξέλθει στις συνεχώς αυξανόμενες ταχύτητες των δικτύων.

2. **Φύλαξη δεδομένων.** Τα δεδομένα που συλλέχθηκαν από το σύστημα μπορεί να χρειαστεί να διατηρηθούν για μήνες, καθώς είναι άγνωστο αν και πότε θα χρειαστούν πληροφορίες για εξέταση. Ωστόσο σε μεσαία και

μεγάλα δίκτυα ο όγκος των δεδομένων είναι τόσο μεγάλος που θα πρέπει να βρεθεί μια χρυσή τομή, ώστε να μειωθούν οι απαιτήσεις σε αποθηκευτικό χώρο χωρίς να θυσιάζονται πολύτιμες πληροφορίες. Επιπρόσθετα, τα δεδομένα που συλλέγονται από τις διάφορες πηγές θα πρέπει να μεταφέρονται σε ένα κεντρικό αποθηκευτικό χώρο, χωρίς όμως αυτό να επιβαρύνει υπερβολικά το δίκτυο.

3. **Ανάκτηση δεδομένων.** Το σύστημα θα πρέπει να εντοπίζει τα στοιχεία-δεδομένα δια μέσου δικτύων ευρείας περιοχής (WAN). Η πρόκληση εδώ βρίσκεται στη δημιουργία πρωτοκόλλων που να εντοπίζουν και να μεταφέρουν τα στοιχεία δια μέσω του Internet.

Κοινωνικό-οικονομικές δυσκολίες-προκλήσεις:

4. **Ιδιωτικότητα.** Η παρακολούθηση των δικτύων και συνεπώς η παρακολούθηση των δεδομένων (προσωπικών και μη) που μεταφέρονται σε αυτά, και η ιδιωτικότητα των χρηστών, είναι δυο παράμετροι εκ διαμέτρου αντίθετοι. Η ανάγκη όμως για δυνατότητες περαιτέρω διερεύνησης, μετά από κάποιο συμβάν σε κάποιο δίκτυο είναι κάτι που δεν μπορεί να αμεληθεί. Για να επέλθει μια ισορροπία ανάμεσα στην ανάγκη για παρακολούθηση των δικτύων και τη διατήρηση της ιδιωτικότητας των χρηστών, απαιτείται η γνώση και η αποδοχή των χρηστών του δικτύου για την παρακολούθηση των δραστηριοτήτων τους.

5. **Οικονομικοί παράγοντες.** Ο αυξανόμενος αριθμός παραβιάσεων ασφάλειας έχει δημιουργήσει ήδη ουσιαστική οικονομική ζημιά σε πολλούς οργανισμούς και επιχειρήσεις. Η ενσωμάτωση δυνατοτήτων δικανικής στις υποδομές των δικτύων θα εισάγει κάποιο επιπλέον κόστος στην επιχείρηση, το οποίο κόστος θα πρέπει να δικαιολογηθεί σε σχέση με τα πλεονεκτήματα που προσφέρει.

6.2 Μελλοντικές επεκτάσεις

Στο σημείο αυτό επισημαίνονται κάποια σημεία στα οποία πρέπει να εστιάσει η μελλοντική έρευνα και στα οποία υστερούν οι τρέχουσες υλοποιήσεις:

- **Χρόνος.** Ο συγχρονισμός και η ακεραιότητα των πληροφοριών της ημερομηνίας και της ώρας, που σχετίζονται με ένα συμβάν, είναι σημαντικοί παράγοντες για ολόκληρη τη δικανική διαδικασία. Περαιτέρω έρευνα σε αυτό το πεδίο είναι ίσως μέγιστης σημασίας, καθώς αποτελεί τον συνδετικό κρίκο στα δεδομένα που συλλέγονται από πολλαπλές πηγές.

- **Απόδοση.** Η ταχύτητα επεξεργασίας και η απόδοση της ανάλυσης, εξαρτώνται σε μεγάλο βαθμό από τον όγκο των δεδομένων. Ο όγκος των δεδομένων που συλλέγεται και προορίζεται για ανάλυση, συχνά είναι αρκετά μεγάλος. Ο λόγος είναι ότι οι περισσότερες πηγές δεδομένων παρότι μπορούν να συνεισφέρουν σημαντικές πληροφορίες, υστερούν στην αποτελεσματικότητα του φιλτραρίσματος των δεδομένων που συνέλεξαν. Για το λόγο αυτό, επιπλέον έρευνα είναι απαραίτητη, για την αύξηση της αποτελεσματικότητας των τεχνικών και το σχεδιασμό εργαλείων με έξυπνες δυνατότητες μείωσης του όγκου των δεδομένων, που προορίζονται για ανάλυση.

- **Πολυπλοκότητα.** Η εστίαση-μετακίνηση του ενδιαφέροντος της ανάλυσης, από τα αυτόνομα υπολογιστικά συστήματα στα δικτυακά περιβάλλοντα για λεπτομερή εξέταση των δεδομένων, αυξάνει σημαντικά το επίπεδο πολυπλοκότητας. Τα εργαλεία που χρησιμοποιούνται για την εξέταση ενός υπολογιστή, δεν μπορούν να χρησιμοποιηθούν σε ένα δικτυακό περιβάλλον με πολλαπλά λειτουργικά συστήματα, πρωτόκολλα, εφαρμογές και μορφές δεδομένων. Θα πρέπει να δημιουργηθούν εργαλεία και να βρεθούν τεχνικές, που να μπορούν να χρησιμοποιηθούν τόσο σε ένα ανεξάρτητο υπολογιστή όσο και σε δικτυακό περιβάλλον.

- **Συσχέτιση.** Η μετατροπή του μεγάλου όγκου των δεδομένων σε χρήσιμα και κατανοητά τμήματα δεδομένων στα οποία μπορεί να γίνει ευκολότερα η

ανάλυση. Η χρήση και η αξιοποίηση τεχνικών εξόρυξης δεδομένων, θα βοηθήσει τους αναλυτές να κατανοήσουν τη σχέση μεταξύ των δεδομένων που προέρχονται από διαφορετικές πηγές.

- **Συλλογή.** Η πραγματοποίηση της ανάλυσης απαιτεί την λεπτομερή εξέταση φιλτραρισμένων δεδομένων, που προέρχονται από διάφορες πηγές, οι οποίες μπορεί να βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες. Τα ζητήματα που πρέπει να αντιμετωπιστούν είναι:

  - **Ποιός** θα συλλέξει τα δεδομένα, καθώς αυτός που θα συλλέξει τα δεδομένα θα πρέπει να είναι άτομο εμπιστοσύνης, ώστε να μην υπάρχει θέμα με την ακεραιότητα των δεδομένων.

  - **Πότε** ή πόσο συχνά θα πρέπει να συλλέγονται τα δεδομένα.

  - **Τι** θα πρέπει να συλλεχθεί. Το ζήτημα αυτό αφορά τις διάφορες μη προτυποποιημένες μορφές δεδομένων που υποστηρίζουν τα διάφορα συστήματα από τα οποία θα συλλεχθούν τα δεδομένα.

- **Νέες τεχνολογίες.** Οι νέες τεχνολογίες που αναδύονται, αναμένεται να δημιουργήσουν νέες προκλήσεις στο πεδίο της δικανικής δικτύων και δίνουν κίνητρα για έρευνα πάνω σε αυτές.

  - Η Ασύρματη τεχνολογία προσθέτει επιπλέον επίπεδα στην ανάλυση, ενσωματώνοντας νέα πρωτόκολλα και υπηρεσίες, τα οποία πρέπει να κατανοηθούν και να ληφθούν υπ’ όψιν. Όπως για παράδειγμα, τον ακριβή εντοπισμό των ασύρματων συσκευών.

  - Η ενσωμάτωση των ενσύρματων υπηρεσιών σε ασύρματες αρχιτεκτονικές θα προσθέσει πολυπλοκότητα. Τα PDA, τα δίκτυα κινητών υπηρεσιών 3G και 4G, καθώς και οι peer-to-peer εφαρμογές, θα πρέπει να μελετηθούν για να διαπιστωθεί η επίδραση τους στη δικανική δικτύων.

6.3 Συμπεράσματα - Επίλογος

Η ασφάλεια στο περιβάλλον του Internet είναι σημαντική, επειδή η αξία των πληροφοριών είναι μεγάλη, αλλά και δύσκολη. Είναι δύσκολη επειδή συνεπάγεται την κατανόηση του χρόνου και του τρόπου με τους οποίους οι συμμετέχοντες χρήστες, υπολογιστές, υπηρεσίες και δίκτυα θα μπορούν να εμπιστευτούν το ένα το άλλο, καθώς και την κατανόηση των τεχνικών λεπτομερειών του υλικού δικτύων και των πρωτοκόλλων. Η ασφάλεια είναι απαραίτητη σε κάθε υπολογιστή και σε κάθε πρωτόκολλο. Ένα αδύναμο σημείο αρκεί για να διακυβεύσει την ασφάλεια ολόκληρου του δικτύου.

Ο ιδιαίτερος χαρακτήρας του Internet, προκύπτει από την ανοχή που διαθέτει σε αναξιόπιστες συνδέσεις, καθώς σχεδιάστηκε έτσι ώστε να υποστηρίζει πολλαπλές εναλλακτικές συνδέσεις μεταξύ των υπολογιστών. Ένα δικτυωμένο σύστημα είναι επιρρεπές σε ένα αριθμό απειλών που προέρχονται από νόμιμους χρήστες του συστήματος αλλά κυρίως από επίδοξους εισβολείς. Σε αυτά, προστίθεται το πρόβλημα επικοινωνίας του δικτύου και της προσπέλασης του από μακρινά μη έμπιστα υπολογιστικά συστήματα. Σε ένα δίκτυο, όσο περισσότερα σημεία πρόσβασης υπάρχουν τόσα περισσότερα πιθανά σημεία επιθέσεων πρέπει να οχυρωθούν.

Η δικανική δικτύων μπορεί να αποδειχθεί ένα χρήσιμο εργαλείο στη διερεύνηση των επιθέσεων σε δίκτυα υπολογιστών. Ένα σύστημα δικανικής δικτύων μπορεί να ανιχνεύσει δραστηριότητες κατάχρησης του δικτύου, να ανακαλύψει πιθανούς κινδύνους μέσα από την ανάλυση των λεπτομερειών των δεδομένων που έχουν συλλεχθεί, να επιταχύνει την αντίδραση στις επιθέσεις του δικτύου, να αυξήσει τις δυνατότητες διερεύνησης και ανεύρεσης στοιχείων.

Η αναγνώριση του επιτιθέμενου δεν είναι ζήτημα πρωταρχικής σημασίας μετά από μια εισβολή του συστήματος. Ωστόσο, οι ερευνητές του δικτύου χρησιμοποιώντας δικανικά εργαλεία μπορούν να συλλέξουν πληροφορίες για τον επιτιθέμενο ώστε να αποτρέψουν μελλοντικές επιθέσεις. Η δικανική ανάλυση απαιτεί εξειδικευμένα εργαλεία με δυνατότητες αποτελεσματικού φιλτραρίσματος του μεγάλου όγκου των δεδομένων που έχουν συλλεχθεί στο δίκτυο και με δυνατότητες απεικόνισης πολλαπλών όψεων των δικτυακών δεδομένων. Ολοκληρωμένα NFAT εργαλεία

και διάφοροι μέθοδοι, όπως η ιχνηλάτηση IP διευθύνσεων, είναι πολύτιμοι σύμμαχοι στην προσπάθεια συλλογής στοιχείων από την κίνηση του δικτύου.

Η εφαρμογή κάποιου μοντέλου δικανικής δικτύων μπορεί να παράσχει καθοδήγηση στην δικανική διαδικασία. Ωστόσο είναι απαραίτητη η προτυποποίηση των μοντέλων και η συμπλήρωση των κενών που πιθανόν να παρουσιάζουν ώστε η δικανική διαδικασία να γίνει πιο αποτελεσματική και να υπάρχει μεγαλύτερη εγκυρότητα των αποτελεσμάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[Ahm05] Ahmad Almulhem , Issa Traore: Experience with Engineering a Network Forensics System, 2005

[Bri02] BRIAN Carrie. Defining Digital Forensics Examination and Analysis Tools, In Digital Research Workshop II, 2002.

[BRO07] Brown, L.T. Christopher, Computer Evidence: Collection and Preservation , Laxmi Publications, 2007.

[Bru05] D.Bruschi, M.Monga, E.Rosti, Trusted Internet Forensics: design of a network forensics appliance, 2005

[Cor02] COREY, V.; etc. Network forensics analysis, Internet Computing, IEEE, Volume: 6 Issue: 6 , Nov.-Dec. 2002 Page(s): 60 –66.

[Erb06] Robert F. Erbacher, Kim Christiansen and Amanda Sundberg, “Visual Network Forensics Techniques and Processes”, June 2006

[Gar01] GARY, P. A Road Map for Digital Forensic Research, Technical Report DTRT0010-01, DFRWS, November 2001.

[IJC08] IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008

[Jou00] Y. Jou, F. Gong, C. Sargor, X. Wu, S. Wu, H. Chang, and F. Wang, "Design and Implementation of a Scalable Intrusion Detection System for the Protection of Network Infrastructure", DARPA Information Survivability Conference and Exposition 2000, Jan 25-27, 2000, Vol. 2, pp 69-83

[Kan06] Panagiotis Kanellis: Digital Crime And Forensic Science in Cyberspace, Idea Group Inc (IGI), 2006

[Kiz05] Joseph M. Kizza: Computer Network Security, Springer, 2005

[Kum06] "Experimentation in Network Forensics", Naveen K. Kumashi, Salman A. Kagzi,Tanya Gupta, Priyanka Bhattacharya, Sanyam Dixit, December 2006

[LEB07] Dee-Ann LeBlanc, Richard Blum, Linux for Dummies, Edition: 8, illustrated, For Dummies, 2007

[Man01] Yanet Manzano and Alec Yasinsac, "Policies to Enhance Computer and Network Forensics", 2nd Annual IEEE Systems, Man, Cybernetic Information Assurance Workshop, June 2001.

[Man02] Yanet Manzano and Alec Yasinsac. (2002) Honeytraps, A network forensic tool (Paper Draft).

[MAR07] Albert J. Marcella, Doug Menendez, Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes, Edition: 2, illustrated, CRC Press, 2007

[MAY06] Mayank R. Gupta , Michael D. Hoeschele , Marcus K. Rogers, Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence Fall 2006, Volume 5, Issue 1

[McH08] John McHugh: Passive network forensics: behavioral classification of network hosts based on connection patterns, 2008

[NIJ08] NIJ, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, 2008, www.ojp.usdoj.gov/nij

[NIS86] NIST: Guide to Integrating Forensic Techniques into Incident Response, SP 800-86

[NIS94] NIST: Guide to Intrusion Detection and Prevention Systems (IDPS), SP 800-94

[Red05] S.Redding, Using Peer-to-Peer technology for Network Forensics, 2005

[Ren04] Ren Wei, “On A Network Forensics Model for Information Security”, 2004

[Ren05] Ren Wei, Hai Jin, “Honeynet based Distributed Adaptive Network Forensics and Active Real Time Investigation”, March 2005

[Sha03] ForNet: A Distributed Forensics Network (2003) Kulesh Shanmugasundaram, Nasir

[SOL04] Michael G. Solomon, Diane Barrett, Neil Broom, Computer forensics jumpstart, Edition: illustrated, John Wiley and Sons, 2004

[Spa03] Ryan Spangler, “Packet Sniffer Detection with AntiSniff”, May 2003

[Vig99] Vigna and Kemmerer, "NetSTAT: A Network-based Intrusion Detection System” "Journal of Computer Security", Volume 7, Issue 1, 1999

Ηλεκτρονικές Πηγές

[E11] http://www.utica.edu/academic/institutes/ecii/ijde/

[E12] http://www.7safe.com/electronic_evidence/

[E13] http://en.wikipedia.org/wiki/Filesystem

[E14] http://www.forensics-intl.com/def2.html

[E15] http://encyclopedia.thefreedictionary.com/Disk+imaging

[E16] http://en.wikipedia.org/wiki/Cryptographic_hash_function

[E17] http://en.wikipedia.org/wiki/Cyclic_redundancy_check

[E18] http://en.wikipedia.org/wiki/Metadata

[E19] http://www.thinkwiki.org/wiki/Hidden_Protected_Area

[E110] http://en.wikipedia.org/wiki/RAID

[E111] http://en.wikipedia.org/wiki/Hex_editor

[E112] http://en.wikipedia.org/wiki/Operating_system

[E113] http://en.wikipedia.org/wiki/Computer_forensics

[E114] http://gcn.com/articles/2006/07/27/special-report--live-forensics-is-the-future-for-law-enforcement.aspx

[E115] http://www.ijofcs.org/webjournal/index.php/ijofcs

[E31] http://www.tcpdump.org/

[E32] http://en.wikipedia.org/wiki/Tcpdump

[E33] http://en.wikipedia.org/wiki/Wireshark

[E34] http://www.wireshark.org/

[E35] http://en.wikipedia.org/wiki/Kismet_(software)

[E36] http://www.kismetwireless.net/

[E37] http://ngrep.sourceforge.net/

[E38] http://www.softpanorama.org/Net/Netutils/ngrep.shtml

[E39] http://www.netstumbler.com/

[E310] http://www.qosient.com/argus/

[E311] http://nsmwiki.org/index.php?title=Argus]

[E312] http://etherape.sourceforge.net/

[E313] http://en.wikipedia.org/wiki/Etherape

[E314] http://www.snort.org/

[E315] http://en.wikipedia.org/wiki/Snort_(software)

[E316] http://www.circlemud.org/~jelson/software/tcpflow/

[E317] http://www.xplico.org/

[E318] http://networkminer.sourceforge.net/

[E319] http://www.breachbytes.com/2008/01/08/computer-forensics-vs-network-forensics/#more-17

[E41] Raul Siles, Wireless Forensics: Tapping the Air - Part One http://www.securityfocus.com/infocus/1884

[E42] Raul Siles, Wireless Forensics: Tapping the Air - Part Two http://www.securityfocus.com/infocus/1885

[E43] “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”. IEEE. June 2003. http://standards.ieee.org/getieee802/download/802.11-1999.pdf,

[E44] www.icardforensics.com/documents/aircapture.pdf

[E45] The Janus Project. http://www.tgdaily.com/2006/08/30/defcon2006_janus_project/

[E46] WLAN-14. AirCapture. http://www.aircapture.net

[E47] Raw Covert. Laurent Butti. 2006. http://rfakeap.tuxfamily.org/#Raw_Covert

[E48] WiFi Advanced Stealth Patches. Laurent Butti and Franck Veysset. 2006. http://rfakeap.tuxfamily.org/#WiFi_Advanced_Stealth_Patches

[E49] http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Veyssett.pdf

Παράρτημα Α - Σενάριο

Σε αυτό το σημείο περιγράφεται ένα παράδειγμα εφαρμογής της δικανικής διαδικασίας, χρησιμοποιώντας πολλαπλές πηγές δεδομένων. Το σενάριο υποθέτει ότι το δίκτυο έχει μολυνθεί από ένα σκουλήκι (worm) και σκοπός είναι να προσδιοριστεί ο τύπος του και τα χαρακτηριστικά του.

Το γραφείο εξυπηρέτησης ενός οργανισμού λαμβάνει πολλά τηλεφωνήματα και μηνύματα παραπόνων, που αφορούν την αργή απόκριση ενός συγκεκριμένου εξυπηρετητή (server). Το γραφείο εξυπηρέτησης ενημερώνει την ομάδα επιτήρησης του δικτύου για τα παράπονα που έλαβε. Το σύστημα ανίχνευσης εισβολών (IDS) του δικτύου ανέφερε αρκετές ασυνήθιστες προειδοποιήσεις (alerts), που αφορούσαν το συγκεκριμένο εξυπηρετητή και ο αναλυτής, ο οποίος εξέτασε τις προειδοποιήσεις πιστεύει ότι είναι ακριβείς. Τα δεδομένα από τις προειδοποιήσεις υποδεικνύουν ότι κάποια ύποπτη δραστηριότητα κατευθύνθηκε προς τον εξυπηρετητή και ο εξυπηρετητής πλέον παράγει πανομοιότυπη δραστηριότητα προς άλλα συστήματα. Η πρώτη υπόθεση του αναλυτή, είναι ότι ένα σκουλήκι εκμεταλλευόμενο κάποια αδυναμία του δικτύου ,έχει μολύνει τον εξυπηρετητή, ο οποίος τώρα προσπαθεί να μολύνει άλλα συστήματα. Η ομάδα επιτήρησης του δικτύου επικοινωνεί με τον υπεύθυνο για την διαχείριση τέτοιων συμβάντων, ώστε να εξετάσει το ενδεχόμενο συμβάν στον εξυπηρετητή.

Σκοπός είναι να προσδιοριστεί ο τύπος του και τα χαρακτηριστικά του σκουληκιού που έχει μολύνει το σύστημα. Αυτές οι πληροφορίες είναι ζωτικής σημασίας για να μπορέσει να γίνει αποτελεσματική αντιμετώπιση του προβλήματος και για την πρόληψη μολύνσεως άλλων συστημάτων. Σε αυτό το στάδιο μπορεί να εξακριβωθεί αν όντως το πρόβλημα προκλήθηκε από κάποιο σκουλήκι ή από κάτι άλλο.

Οι πληροφορίες που έχουν καταγραφεί και αφορούν το συμβάν μπορεί να βρίσκονται σε διάφορες πηγές. Πρώτα εξετάζονται οι πηγές που έχουν τη μεγαλύτερη πιθανότητα να περιέχουν στοιχεία, με βάση προηγούμενη εμπειρία σε παρόμοιες καταστάσεις. Για παράδειγμα, αφού το IDS ανίχνευσε την ύποπτη δραστηριότητα, πιθανότατα και άλλες πηγές που παρακολουθούσαν το ίδιο τμήμα του δικτύου θα περιέχουν σχετικά με το συμβάν δεδομένα. Αν υπάρχει διαθέσιμο

λογισμικό SEM (security event management) ή NFAT, τα οποία συγκεντρώνουν τα δεδομένα από τις διάφορες πηγές, τότε οι πληροφορίες μπορούν να εξαχθούν χρησιμοποιώντας κάποια ερωτήματα (queries). Αν δεν υπάρχει κάποιο εργαλείο, το οποίο να συγκεντρώνει τα δεδομένα από όλες τις πηγές, τότε θα πρέπει να εξεταστεί η κάθε πηγή χωριστά:

- **Network IDS.** Από τη στιγμή που το IDS ανίχνευσε το συμβάν, είναι πιθανό να έχει καταγράψει κάποια δεδομένα με τα βασικά χαρακτηριστικά της δραστηριότητας του δικτύου. Στην χειρότερη περίπτωση, τα δεδομένα θα προσδιορίζουν τον εξυπηρετητή που δέχτηκε την επίθεση και τον αριθμό θύρας, ο οποίος μπορεί να υποδείξει ποια υπηρεσία βρισκόταν στο στόχαστρο της επίθεσης. Η αναγνώριση της υπηρεσίας είναι σημαντική, ώστε να βρεθεί η αδυναμία του συστήματος και για να αποτραπούν παρόμοια περιστατικά σε άλλα συστήματα. Κάποια IDS ίσως καταγράψουν επιπλέον πληροφορίες που αφορούν δεδομένα των εφαρμογών (π.χ. κεφαλίδες E-mail).

- **Network-Based Firewall.** Ένα firewall συνήθως ρυθμίζεται να καταγράφει τις προσπάθειες σύνδεσης που μπλοκαρίστηκαν μαζί με την πόρτα και την IP προορισμού. Συνεπώς, το firewall πιθανόν να έχει καταγράψει τη δραστηριότητα του σκουληκιού. Μερικά σκουλήκια προσπαθούν να εκμεταλλευτούν τις αδυναμίες πολλαπλών υπηρεσιών και έτσι το firewall μπορεί να έχει καταγράψει ότι το σκουλήκι προσπάθησε να συνδεθεί σε τουλάχιστον τέσσερις πόρτες αλλά μπλόκαρε μόνο τις τρείς. Αυτή η πληροφορία μπορεί να φανεί χρήσιμη στην αναγνώριση του σκουληκιού. Αν το firewall έχει ρυθμιστεί να καταγράφει τις συνδέσεις που επιτράπηκαν, τότε οι πληροφορίες μπορεί να υποδείξουν ποιοι υπολογιστές δέχθηκαν κίνηση από το σκουλήκι ή μολύνθηκαν και αναπαράγουν την κίνηση του σκουληκιού. Αυτό είναι χρήσιμο στις περιπτώσεις που το IDS δεν παρακολουθεί όλη την κίνηση που φτάνει στο firewall. Άλλες συσκευές του δικτύου, όπως οι δρομολογητές, από τις οποίες πέρασε κίνηση που δημιούργησε το σκουλήκι, μπορεί να έχουν καταγράψει παρόμοιες πληροφορίες με αυτές του firewall.

- **Host IDS και Firewall.** IDS και Firewall που βρίσκονται στα μολυσμένα συστήματα μπορεί να περιέχουν περισσότερες λεπτομέρειες, όπως αλλαγές σε αρχεία και στις ρυθμίσεις του υπολογιστή. Ωστόσο, πολλά σκουλήκια απενεργοποιούν τους μηχανισμούς ασφαλείας του εκάστοτε υπολογιστή και διαγράφουν τα αρχεία καταγραφής που έχουν δημιουργήσει. Αν δεν υπάρχει κάποιος κεντρικός εξυπηρετητής στον οποίο να προωθούνται αντίγραφα από τα αρχεία καταγραφής τότε πιθανότατα οι πληροφορίες αυτές να έχουν χαθεί.

- **Αρχεία καταγραφής των εφαρμογών.** Αν το σκουλήκι χρησιμοποίησε κάποια κοινά πρωτόκολλα, όπως το HTTP ή SMTP, τότε πληροφορίες μπορεί να βρίσκονται στα αρχεία καταγραφής του εξυπηρετητή εφαρμογών ή στον proxy server. Τα αρχεία καταγραφής των εφαρμογών περιέχουν λεπτομέρειες και χαρακτηριστικά της κίνησης που αφορούν συγκεκριμένες εφαρμογές.

Σκοπός αυτής της αρχικής διερεύνησης είναι η συλλογή πληροφοριών, ώστε να αναγνωριστούν κάποια βασικά χαρακτηριστικά του σκουληκιού. Ο αναλυτής μπορεί να αναζητήσει για γνωστές υπογραφές σκουληκιών, στις βάσεις δεδομένων διαφόρων κατασκευαστών αντιϊκών προγραμμάτων, όπου μπορεί να βρει αρκετές πληροφορίες σχετικές με τη μετάδοση τους, τα προβλήματα που δημιουργούν και το πώς μπορεί να περιοριστεί και να εξαλειφτεί η δράση τους.

Για την αναζήτηση ακόμα περισσότερων πληροφοριών, ο αναλυτής μπορεί να εξετάσει ένα μολυσμένο υπολογιστή. Πιο συγκεκριμένα, να εξετάσει τις συνδέσεις που έχουν επιτευχθεί για τυχόν ασυνήθιστες συνδέσεις (π.χ. χρήση απρόσμενων αριθμών πόρτας ή χρήση μεγάλου αριθμού πορτών). Επίσης ο αναλυτής μπορεί να συλλέξει την κίνηση που δημιουργήθηκε από το σκουλήκι χρησιμοποιώντας ένα packet sniffer.

Γενικά, η εισβολή ενός σκουληκιού στο σύστημα, απαιτεί γρήγορη αντίδραση ώστε να αποφευχθεί η μόλυνση άλλων συστημάτων. Επιπλέον, τα σκουλήκια μερικές φορές ανοίγουν κάποιες πόρτες (backdoors) ή εγκαθιστούν κάποια άλλα εργαλεία, για να επιτρέψουν την απομακρυσμένη πρόσβαση στο σύστημα, το οποίο μπορεί

να επιφέρει μεγαλύτερες συνέπιες. Μερικοί υπεύθυνοι ασφαλείας επιλέγουν να αποσυνδέσουν το μολυσμένο σύστημα από το δίκτυο αντι να συλλέξουν τα δεδομένα από αυτό. Με αυτόν τον τρόπο όμως γίνεται δυσκολότερη η αναγνώριση του σκουληκιού και ο προσδιορισμός των συνεπειών που είχε στο σύστημα.

Παράρτημα Β - Γλωσσάριο

Analysis: Το τρίτο στάδιο της δικανικής δικτύων και υπολογιστών, το οποίο περιλαμβάνει τη χρήση μεθόδων και τεχνικών για την εξαγωγή χρήσιμων πληροφοριών.

Anti-Forensic: Το σύνολο των τεχνικών που χρησιμοποιούνται για την απόκρυψη και την καταστροφή των δεδομένων από ένα σύστημα, ώστε να μην μπορέσουν να ανακτηθούν από άλλους.

Bit Stream Imaging: Η δημιουργία ενός bit προς bit αντιγράφου ενός μέσου, το οποίο περιλαμβάνει το free space και το slack space. Γνωστό και ως disk imaging.

Cluster: Ένα γκρουπ από γειτονικούς sectors.

Collection: Το πρώτο στάδιο της δικανικής δικτύων και υπολογιστών, το οποίο περιλαμβάνει την αναγνώριση, την καταγραφή και την απόκτηση δεδομένων από πιθανές πηγές, διατηρώντας μια μεθοδολογία ώστε να διατηρείται η ακεραιότητα των δεδομένων.

Data: Διακριτά τμήματα ψηφιακής πληροφορίας, διαμορφωμένα με ένα συγκεκριμένο τρόπο-μορφή.

Digital Forensics: Η εφαρμογή της επιστήμης στην αναγνώριση, τη συλλογή, την εξέταση και την ανάλυση των δεδομένων, διατηρώντας παράλληλα τη συνοχή και την ακεραιότητα των δεδομένων.

Directory: Οργανωτικές δομές που χρησιμοποιούνται για την ομαδοποίηση αρχείων.

Disk Imaging: Η δημιουργία ενός bit προς bit αντιγράφου ενός μέσου, το οποίο περιλαμβάνει το free space και το slack space. Γνωστό και ως bit stream imaging.

Disk-to-Disk Copy: Η αντιγραφή των περιεχομένων ενός μέσου, κατευθείαν σε ένα άλλο μέσο.

Disk-to-File Copy: Η αντιγραφή των περιεχομένων ενός μέσου, σε ένα λογικό αρχείο δεδομένων.

Examination: Το δεύτερο στάδιο της δικανικής δικτύων και υπολογιστών, το οποίο περιλαμβάνει την αυτοματοποιημένη ή χειροκίνητη επεξεργασία μεγάλων όγκων συλλεγμένων δεδομένων, ώστε να εξαχθούν τα δεδομένα που ενδιαφέρουν διατηρώντας παράλληλα την ακεραιότητα των δεδομένων.

False Negative: Λανθασμένη κατηγοριοποίηση κακόβουλης δραστηριότητας ως ήπια.

False Positive: Λανθασμένη κατηγοριοποίηση ήπιας δραστηριότητας ως κακόβουλη.

File: Μια συλλογή λογικά ομαδοποιημένων πληροφοριών, σε μια οντότητα με μοναδικό όνομα.

File Allocation Unit: Μια ομάδα γειτονικών sectors, γνωστή και ως cluster.

File Header: Δεδομένα που περιέχονται σε ένα αρχείο, τα οποία περιέχουν πληροφορίες αναγνώρισης του αρχείου και μεταδεδομένα, με πληροφορίες για τα περιεχόμενα του αρχείου.

Filename: Ένα μοναδικό όνομα που αναφέρεται σε ένα αρχείο.

Filesystem: Μια μέθοδος για την ονομασία, την αποθήκευση, την οργάνωση και την πρόσβαση των αρχείων σε λογικούς τόμους.

Forensically Clean: Ένα ψηφιακό μέσο το οποίο έχει υποστεί ψηφιακό καθαρισμό και δεν περιέχει κανενός είδους δεδομένα.

Free Space: Μια περιοχή του δίσκου ή της μνήμης, στην οποία δεν έχουν τοποθετηθεί δεδομένα..

Logical Backup: Ένα αντίγραφο των καταλόγων και των αρχείων ενός λογικού τόμου.

Logical Volume: Ένα τμήμα ή μια συλλογή τμημάτων που συμπεριφέρονται σαν μια οντότητα μορφοποιημένη με ένα filesystem.

Message Digest: Ένα μήνυμα κατακερματισμού (hash), το οποίο μοναδικά επαληθεύει τα δεδομένα. Η αλλαγή ενός και μόνο bit στα δεδομένα, έχει ως αποτέλεσμα ένα τελείως διαφορετικό μήνυμα.

Metadata: Δεδομένα που προσδιορίζουν τα δεδομένα. Στα filesystems για παράδειγμα, τα metadata παρέχουν πληροφορίες για τα περιεχόμενα ενός αρχείου.

Network Address Translation: Η διαδικασία αντιστοίχισης των διευθύνσεων ενός δικτύου σε διευθύνσεις ενός άλλου δικτύου.

Network Intrusion Detection System: Λογισμικό, το οποίο ελέγχει την κίνηση του δικτύου για την ανίχνευση ύποπτης δραστηριότητας και την καταγραφή σχετικών πληροφοριών.

Network Traffic: Το σύνολο των δεδομένων επικοινωνίας, ενσύρματων ή ασύρματων δικτύων, που ανταλλάσσονται μεταξύ υπολογιστών.

Non-Volatile Data: Δεδομένα τα οποία διατηρούνται σε ένα υπολογιστικό σύστημα ακόμα και μετά τη διακοπή της τροφοδοσίας ρεύματος.

Normalize: Η διαδικασία με την οποία διαφορετικά μορφοποιημένα δεδομένα, μετατρέπονται σε μια πρότυπη μορφή.

Operating System: Ένα πρόγραμμα το οποίο εκτελείται σε ένα υπολογιστή και παρέχει την πλατφόρμα πάνω στην οποία, άλλα προγράμματα μπορούν να εκτελεστούν.

Packet: Η λογική μονάδα στην επικοινωνία δικτύων, η οποία παράγεται από το επίπεδο μεταφοράς

Packet Sniffer: Λογισμικό, το οποίο παρακολουθεί τη δικτυακή κίνηση σε ενσύρματα ή ασύρματα δίκτυα και συλλαμβάνει τα πακέτα.

Partition: Το λογικό τμήμα ενός μέσου, το οποίο λειτουργεί σαν να ήταν φυσικά διαχωρισμένο από τα υπόλοιπα λογικά τμήματα του μέσου.

Process: Ένα πρόγραμμα που εκτελείται.

Protocol Analyzer: Λογισμικό, το οποίο μπορεί να συναρμολογήσει τις ροές από τα πακέτα και να αποκωδικοποιήσει τις επικοινωνίες που χρησιμοποιούν διάφορα πρωτόκολλα.

Proxy: Λογισμικό, το οποίο λαμβάνει μια αίτηση από έναν υπολογιστή-πελάτη (client) και στη συνέχεια αποστέλλει μια αίτηση εκ μέρους του υπολογιστή-πελάτη, στον επιθυμητό υπολογιστή.

Remote Access Server: Συσκευή, η οποία πραγματοποιεί συνδέσεις σε δίκτυα.

Reporting: Το τελευταίο στάδιο της δικανικής δικτύων και υπολογιστών, το οποίο περιλαμβάνει την αναφορά των αποτελεσμάτων της ανάλυσης.

Sector: Η μικρότερη μονάδα που μπορεί να προσπελαστεί σε ένα μέσο.

Security Event Management Software: Λογισμικό, το οποίο εισάγει πληροφορίες που αφορούν συμβάντα ασφαλείας, από πολλαπλές πηγές, κανονικοποιεί τα δεδομένα και συσχετίζει τα συμβάντα από τις διάφορες πηγές.

Slack Space: Αχρησιμοποίητος χώρος σε ένα file allocation block ή σελίδα μνήμης, ο οποίος μπορεί να περιέχει γειτονικά δεδομένα.

Steganography: Η ενσωμάτωση δεδομένων μέσα σε άλλα δεδομένα, με σκοπό την απόκρυψη τους.

Subdirectory: Ένας κατάλογος που περιέχεται μέσα σε ένα άλλο κατάλογο.

Volatile Data: Δεδομένα τα οποία διατηρούνται σε ένα υπολογιστικό σύστημα όσο υπάρχει τροφοδοσία ρεύματος. Μετά την διακοπή της τροφοδοσίας χάνονται.

Wiping: Η επανεγγραφή ενός μέσου ή τμήματος του μέσου, με τυχαίες ή σταθερές ακολουθίες από 0 και 1, ώστε να παρεμποδιστεί η συλλογή των δεδομένων.

Write-Blocker: Ένα εργαλείο, το οποίο εμποδίζει την εγγραφή ή την τροποποίηση όλων των αποθηκευτικών μέσων που είναι συνδεδεμένα σε ένα υπολογιστή.

Παράρτημα Γ - Ακρωνύμια

ADS: Alternate Data Stream

ARIN: American Registry for Internet Numbers

ARP: Address Resolution Protocol

ASCII: American Standard Code for Information Interchange

BIOS: Basic Input/Output System

CD: Compact Disc

CD-R: CD-Recordable

CD-ROM: CD-Read Only Memory

CD-RW: CD-Rewritable

CDFS: CD File System

CFTT: Computer Forensics Tool Testing

CMOS: Complementary Metal Oxide Semiconductor

CVE: Common Vulnerabilities and Exposures

DDoS: Distributed Denial of Service

DHCP: Dynamic Host Configuration Protocol

DLL: Dynamic Link Library

DNS: Domain Name System

DVD: Digital Video Disc or Digital Versatile Disc

DVD-R: DVD-Recordable

DVD-ROM: DVD Read Only Memory

DVD-RW: DVD-Rewritable

ESP: Encapsulating Security Payload

ext2fs: Second Extended Filesystem

ext3fs: Third Extended Filesystem

FAT: File Allocation Table

F.I.R.E.: Forensic and Incident Response Environment

FTP: File Transfer Protocol

GB: Gigabyte

GUI: Graphical User Interface

HFS: Hierarchical File System

HPA: Host Protected Area

HPFS: High-Performance File System

HTCIA: High Technology Crime Investigation Association

HTTP: Hypertext Transfer Protocol

IACIS: International Association of Computer Investigative Specialists

ICMP: Internet Control Message Protocol

ID: Identification

IDE: Integrated Drive Electronics

IDS: Intrusion Detection System

IGMP: Internet Group Management Protocol

IM: Instant Messaging

IMAP: Internet Message Access Protocol

IOS: Internetwork Operating System

IP: Internet Protocol

IPsec: Internet Protocol Security

IR: Interagency Report

IRC: Internet Relay Chat

IRQ: Interrupt Request Line

ISO: International Organization for Standardization

ISP: Internet Service Provider

IT: Information Technology

ITL: Information Technology Laboratory

JPEG: Joint Photographic Experts Group

KB: Kilobyte

MAC: Media Access Control

MAC: Modification, Access, and Creation

MB: Megabyte

MD: Message Digest

MMC: Multimedia Card

MO: Magneto Optical

MS-DOS: Microsoft Disk Operating System

NAT: Network Address Translation

NFAT: Network Forensic Analysis Tool

NFS: Network File Sharing

NIC: Network Interface Card

NTFS: Windows NT File System

NTP: Network Time Protocol

OS: Operating System

PCMCIA: Personal Computer Memory Card International Association

PDA: Personal Digital Assistant

POP3: Post Office Protocol 3

RAID: Redundant Arrays of Inexpensive Disks

RAM: Random Access Memory

RFC: Request for Comment

SAM: Security Account Manager

SCSI: Small Computer System Interface

SD: Secure Digital

SDMI: Secure Digital Music Initiative

SEM: Security Event Management

SFTP: Secure FTP

SHA-1: Secure Hash Algorithm 1

SIP: Session Initiation Protocol

SMB: Server Message Block

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SSH: Secure Shell

SSL: Secure Sockets Layer

TB: Terabytes

TCP: Transmission Control Protocol

TCP/IP: Transmission Control Protocol/Internet Protocol

UDF: Universal Disk Format

UDP: User Datagram Protocol

UFS: UNIX File System

UPS: Uninterruptible Power Supply

URL: Uniform Resource Locator

USB: Universal Serial Bus

VoIP: Voice Over IP

VPN: Virtual Private Network

Παράρτημα Δ – Κώδικας εφαρμογής

```
/* @author Gialouris Konstantinos
 * @version 1.00 13/12/2009
 */
import java.io.*;
import java.util.*;
import org.jdom.*;
import org.jdom.input.SAXBuilder;
//GUI
import java.awt.*;
import java.awt.event.*;
import javax.swing.*;
//DataBase
import java.sql.*;
import java.util.Vector;

public class DPacketViewer extends JFrame {

    Container cp;
    JTable table;
    JPanel panel;
    JScrollPane scrollPane;


    //Bar and menus
    JMenuBar menuBar;
    JMenu fileMenu, viewMenu, sortMenu, helpMenu;
    JMenuItem fileOpen, fileExit, infoItem;
    JRadioButtonMenuItem sortItems[]; // sort menu items
    ButtonGroup sortButtonGroup; // manages sort menu items
    MenuItemHandler handler;
    String fileNameInner = "";

    //Gia tin me8odo eisafwgis arxeiou XML sto programma
    JFileChooser chooser = new JFileChooser();

    //Packet Info to DataBase
    int     Frame_Number =0;
    String FrameNo = "";
    String Frame_Protocols = "";
    String MAC_Source = "";
    String MAC_Destination = "";
    String IP_Source = "";
    String IP_Destination = "";
    String TCP_UDP_Source_Port = "";
    String TCP_UDP_Destination_Port = "";
    String sql;
```

```
46      //Create connection
47      static String sourceURL;
48      static Connection dbconnection;
49      static Statement statement;
50      static ResultSet result;
51
52      //Gia tin ta3inomisi
53      String querySortedByFrameNum  =
54        "SELECT * FROM packetInfo "
55          +"ORDER BY Frame_Number";
56      String querySortedByMacSource =
57        "SELECT * FROM packetInfo "
58          +"ORDER BY MAC_Source DESC";
59      String querySortedByMacDest   =
60        "SELECT * FROM packetInfo "
61          +"ORDER BY MAC_Destination DESC";
62      String querySortedByIpSource  =
63        "SELECT * FROM packetInfo "
64          +"ORDER BY IP_Source";
65      String querySortedByIpDest    =
66        "SELECT * FROM packetInfo "
67          +"ORDER BY IP_Destination";
68      String querySortedByPortSource=
69        "SELECT * FROM packetInfo "
70          +"ORDER BY TCP_UDP_Source_Port DESC";
71      String querySortedByPortDest  =
72        "SELECT * FROM packetInfo "
73          +"ORDER BY TCP_UDP_Destination_Port DESC";
74      String resultsQuery =
75        "SELECT * FROM packetInfo "
76          +"ORDER BY Frame_Number";
```

```
78      Vector<Vector<String>> dataVector;
79      dataVector = new Vector<Vector<String>>();
80      Vector<String> header; //used to store data header
81  //-----------------------------------------------
82  public DPacketViewer() {
83
84      super("GUI Packet Manager" );
85      handler = new MenuItemHandler();
86      cp = getContentPane();
87
88      //Dimiourgia Menu
89      menuBar = new JMenuBar();
90          //Menu File----
91          fileMenu = new JMenu("File");
92              fileOpen = new JMenuItem("Open file");
93              fileOpen.addActionListener( handler );
94
95              fileExit =new JMenuItem("Exit");
96              fileExit.addActionListener( handler );
97          fileMenu.add(fileOpen);
98          fileMenu.add(fileExit);
99
100         //Menu View----
101         viewMenu = new JMenu( "View" );
```

```
102     // pinakas me ta SORT OPTIONS
103     String sortOptions[] = {
104                               "Frame Number",
105                               "MAC Destination",
106                               "MAC Source",
107                               "IP Source",
108                               "IP Destination",
109                               "Source Port",
110                               "Destination Port"
111                             };
112     //Ypo menu tou View
113     sortMenu = new JMenu( "Sort by" );
114     // radio button menu items for sort options
115     sortItems = new JRadioButtonMenuItem[ sortOptions.length ];
116     sortButtonGroup = new ButtonGroup();
117     // handler for sort Options
118     MenuItemHandler itemHandler = new MenuItemHandler();
119     // create sort radio button menu items
120     for ( int count = 0; count < sortOptions.length; count++ )
121     {
122     sortItems[count]=new JRadioButtonMenuItem(sortOptions[count]);
123     sortMenu.add( sortItems[ count ] ); // add item to sort menu
124     sortButtonGroup.add( sortItems[ count ] ); // add to group
125     sortItems[ count ].addActionListener( itemHandler );
126     } // END FOR
127
128     sortItems[ 0 ].setSelected( true ); // select first sort item
129     viewMenu.add( sortMenu ); // add sort menu to view menu
```

```
131         //Menu Help----
132         helpMenu = new JMenu( "Help" );
133             infoItem = new JMenuItem( "Info" );
134             infoItem.addActionListener( handler );
135         helpMenu.add( infoItem );
136
137     //Pros8iki twn menu sti bara
138     menuBar.add(fileMenu);
139     menuBar.add(viewMenu);
140     menuBar.add(helpMenu);
141
142     //Topo8etisi stoixeiwn
143     panel = new JPanel( new BorderLayout() );
144     table = new javax.swing.JTable();
145     scrollPane = new JScrollPane(table);
146     cp.add(scrollPane, BorderLayout.CENTER);
147     cp.add(panel,BorderLayout.SOUTH);
148     setJMenuBar(menuBar);
149
150 }//END DOMHTHS DPacketViewer
```

```
151 public void getData(String resultsQuery) throws Exception  {
152
153     result = statement.executeQuery( resultsQuery );
154
155     while(result.next())  {
156         Vector<String> data = new Vector<String>();
157         data.add(result.getString(1)); //Frame Number
158         data.add(result.getString(2)); //Protocols
159         data.add(result.getString(3)); //MAC Destination
160         data.add(result.getString(4)); //MAC Source
161         data.add(result.getString(5)); //IP Source
162         data.add(result.getString(6)); //IP Destination
163         data.add(result.getString(7)); //Port Source
164         data.add(result.getString(8)); //Port Destination
165         dataVector.add(data);
166     }
167          //create header for the table
168          header = new Vector<String>();
169          header.add("Frame Number");
170          header.add("Frame Protocols");
171          header.add("MAC Destination");
172          header.add("MAC Source");
173          header.add("IP Source");
174          header.add("IP Destination");
175          header.add("Source Port");
176          header.add("Destination Port");
177
178          table.setModel(new javax.swing.table.DefaultTableModel(
179             dataVector,header) );
180          scrollPane.setViewportView(table);
181          cp.add(scrollPane, BorderLayout.CENTER);
182
183  } //END METHOD getData ----
```

```
184 public void processElement( Element el ){
185
186     String elementName = el.getName();
187     String attrValue = el.getAttributeValue( "name" );
188     //anadromi gia to epomeno Element
189     try{
190         if (attrValue.equals("frame.number") ) {
191             FrameNo = el.getAttribute("show").getValue();
192             Frame_Number = Integer.parseInt(FrameNo);
193         } else if( attrValue.equals("frame.protocols") ){
194             Frame_Protocols = el.getAttribute("show").getValue();
195         } else if( attrValue.equals("eth.dst") ){
196             MAC_Destination = el.getAttribute("show").getValue();
197         } else if(attrValue.equals("eth.src")){
198             MAC_Source = el.getAttribute("show").getValue();
199         } else if ( attrValue.equals("arp") ){
200
201             IP_Source = "";
202             IP_Destination= "";
203             TCP_UDP_Source_Port = "";
204             TCP_UDP_Destination_Port = "";
```

```
206             //insert sti database
207             sql = "INSERT INTO packetInfo "
208             + "(Frame_Number, Frame_Protocols,"
209             + "MAC_Destination,MAC_Source,"
210             + "IP_Source,IP_Destination,"
211             + "TCP_UDP_Source_Port,"
212             + "TCP_UDP_Destination_Port ) "
213             + "VALUES ('"
214             + Frame_Number+"','"
215             + Frame_Protocols+"','"
216             + MAC_Destination+ "','"
217             + MAC_Source+ "','"
218             + IP_Source+ "','"
219             + IP_Destination+ "','"
220             + TCP_UDP_Source_Port+ "','"
221             + TCP_UDP_Destination_Port+"' );" ;
222
223             try {
224                 statement.executeUpdate( sql );
225             }
226             catch(Exception e){ }
```

```
228         } else if(attrValue.equals("ip.src")){
229             IP_Source = el.getAttribute("show").getValue();
230         } else if(attrValue.equals("ip.dst")){
231             IP_Destination = el.getAttribute("show").getValue();
232         } else if( attrValue.equals("tcp.srcport")||
233                    attrValue.equals("udp.srcport") ){
234             TCP_UDP_Source_Port=el.getAttribute("show").getValue();
235         } else if ( attrValue.equals("tcp.dstport")||
236                     attrValue.equals("udp.dstport") ){
237         TCP_UDP_Destination_Port=el.getAttribute("show").getValue();
238
239             //insert sti database
240             sql = "INSERT INTO packetInfo "
241             + "(Frame_Number, Frame_Protocols, MAC_Destination,"
242             + "MAC_Source,IP_Source,IP_Destination,"
243             + "TCP_UDP_Source_Port,TCP_UDP_Destination_Port ) "
244             + "VALUES ('"
245             + Frame_Number+"','"
246             + Frame_Protocols+"','"
247             + MAC_Destination+ "','"
248             + MAC_Source+ "','"
249             + IP_Source+ "','"
250             + IP_Destination+ "','"
251             + TCP_UDP_Source_Port+ "','"
252             + TCP_UDP_Destination_Port+"' );" ;
253
254             try {
255                 statement.executeUpdate( sql );
256             }catch(Exception e){    }
257         }
258     } catch(Exception e) {  }
```

```
258     } catch(Exception e) {  }
259
260         java.util.List mixedContent = el.getContent();
261         Iterator iter = mixedContent.iterator();
262
263         while ( iter.hasNext() ) {
264             Object obj = iter.next();
265
266             if (obj instanceof Element) {
267                 processElement( (Element)obj );
268             }
269         }//END while
270 }//END METHOD processElement----------------------
271
272 public void execute(String xmlfile)
273 throws FileNotFoundException,IOException,JDOMException {
274
275     DPacketViewer.MenuItemHandler obj;
276     obj = new DPacketViewer().new MenuItemHandler();
277     String OnomaArxeiou = xmlfile;
278
279     SAXBuilder builder = new SAXBuilder();
280     Document doc=builder.build(new FileInputStream(OnomaArxeiou));
281
282     processElement(doc.getRootElement());
283
284 }//END of METHOD execute--------------------------
```

```
286 public static void connectToDB(){
287
288     try
289     {
290       Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
291       sourceURL = new String("jdbc:odbc:packetDataBase");
292       dbconnection = DriverManager.getConnection(sourceURL);
293       statement = dbconnection.createStatement();
294     }
295     catch( ClassNotFoundException e){ }
296     catch( SQLException ex ){   }
297 }//END of METHOD connectToDB ---
298 //MAIN-------------------------
299 public static void main ( String args[] )
300 throws FileNotFoundException,IOException,JDOMException,SQLException{
301
302     DPacketViewer app = new DPacketViewer();
303     app.addWindowListener( new Close_Window() );
304     app.setSize(900,400);
305     app.setVisible(true);
306
307     connectToDB();
308 }//END MAIN-----------------------------------
```

```
309 //-----INNER CLASS------------------------------
310 class MenuItemHandler implements ActionListener  {
311
312  public void actionPerformed ( ActionEvent e)  {
313
314     String resetTable = "DELETE FROM packetInfo";
315
316 //--Sorting--
317     if ( sortItems[ 0 ].isSelected() ) {
318         resultsQuery = querySortedByFrameNum;
319         try {
320             dataVector.clear();
321             getData(resultsQuery);
322         }catch( Exception excep) {  }
323     }
324     else if( sortItems[ 1 ].isSelected() ) {
325         resultsQuery = querySortedByMacSource;
326         try {
327             dataVector.clear();
328             getData(resultsQuery);
329         }catch( Exception excep) {  }
330     }
331     else if( sortItems[ 2 ].isSelected() ) {
332         resultsQuery = querySortedByMacDest;
333         try {
334             dataVector.clear();
335             getData(resultsQuery);
336         }catch( Exception excep) {  }
337     }
338     else if( sortItems[ 3 ].isSelected() ) {
339         resultsQuery = querySortedByIpSource;
340         try {
341             dataVector.clear();
342             getData(resultsQuery);
343         }catch( Exception excep) {  }
344     }
345     else if( sortItems[ 4 ].isSelected() ) {
346         resultsQuery = querySortedByIpDest;
347         try {
348             dataVector.clear();
349             getData(resultsQuery);
350         }catch( Exception excep) {  }
351     }
352     else if( sortItems[ 5 ].isSelected() ) {
353         resultsQuery = querySortedByPortSource;
354         try {
355             dataVector.clear();
356             getData(resultsQuery);
357         }catch( Exception excep) {  }
358     }
```

```
359     else {
360         resultsQuery = querySortedByPortDest;
361         try {
362             dataVector.clear();
363             getData(resultsQuery);
364         }catch( Exception excep) {  }
365     }
366 //--Sorting--
367 
368     if(e.getSource() == fileExit) {//Epilogi EXIT
369 
370         try { // CLOSE CONNECTION
371             //Adeiasma basis
372             statement.executeUpdate( resetTable );
373             dbconnection.close();
374             System.out.println("Connection Closed");
375         }
376         catch( Exception excep) {}
377 
378         System.exit(0);
379     }
380     else if( e.getSource() == infoItem){
381         JOptionPane.showMessageDialog(null,
382              "Αυτη η εφαρμογή εισάγει "
383             +"ενα XML αρχείο με δικτυακά\n"
384             +"δεδομένα που συλλέχθηκαν απο ενα"
385             +" packet sniffer και\n"
386             +"τα εμφανίζει ομαδοποιημένα και "
387             +"με δυνατότητες ταξινόμησης.",
388         "About this program",JOptionPane.PLAIN_MESSAGE);
389     }
```

```
390     else if( e.getSource() == fileOpen) {
391 
392          chooser.showOpenDialog(null);
393          File xmlFile     = chooser.getSelectedFile();
394          fileNameInner = chooser.getName( xmlFile );
395 
396         if( xmlFile.isFile() ){
397             try {
398                 statement.executeUpdate( resetTable );
399                 dataVector.clear();
400                 execute(fileNameInner);
401                 getData(resultsQuery);
402             }catch( Exception excep) {
403                 Object[] options = { "OK", "CANCEL" };
404                 JOptionPane.showOptionDialog(null,
405                     "You should select an XML file",
406                     "Warning",JOptionPane.DEFAULT_OPTION,
407                     JOptionPane.WARNING_MESSAGE,null,
408                     options, options[0]);
409             }
410         }
411 
412     }//END ELSE IF
413  }//END OF METHOD actionPerformed
414 }//END OF INNER CLASS MenuItemHandler
415 }//END CLASS DPacketViewer
```

```
416 //OUTTER CLASS
417 //Klasi gia ton termatismo tiw efarmogis
418 //me to kleisimo tou para8irou
419 class Close_Window extends WindowAdapter {
420
421         public void windowClosing ( WindowEvent e) {
422             System.exit(0);
423         }
424 }//END OF CLASS Close_Window
```