Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Μεταπτυχιακής εργασίας	**«Ανασκόπηση και περιγραφή των μεθοδολογιών, προτύπων και εργαλείων που χρησιμοποιούνται για την ανάλυση ψηφιακών πειστηρίων διαδικτυακών υπηρεσιών (Web Services Forensics). Επίδειξη κυριοτέρων ανοιχτών εργαλείων με συγκεκριμένες περιπτώσεις χρήσης»** _____ **"Study and description of methodologies, standard processes and tools which are used to analyze Forensics over Web Services. Demonstration of the main open source tools for specific use case"**
Ονοματεπώνυμο	**Παπουτσής Δημήτριος**
Αριθμός Μητρώου	**ΜΠΣΠ/ 11034**
Επιβλέπων καθηγητής	**Πολέμη Νινέτα, Αναπληρώτρια Καθηγήτρια**

Ημερομηνία Παράδοσης: **Μάιος 2015**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα
Πολέμη Νινέτα	Κοτζανικολάου Παναγιώτης	Πατσάκης Κωνσταντίνος
Αναπληρώτρια Καθηγήτρια	Λέκτορας	Λέκτορας

Περίληψη

Στην παρούσα μεταπτυχιακή διατριβή γίνεται θεωρητική περιγραφή των θεμελιωδών αρχών της «Δικανικής Πληροφορικής», καθώς και πειραματική παρουσίαση των τεχνικών στοιχείων που απαρτίζουν την εν λόγω επιστήμη. Αρχικά θα γίνει αναφορά στους ορισμούς, τις έννοιες που απαρτίζουν την «Δικανική Πληροφορική. Θα δοθεί σύντομη περιγραφή του οριζόμενου νομοθετικού πλαισίου, μέσω του οποίου παρέχονται τα στοιχεία στις Δικαστικές αρχές έχοντας σαν στόχο τη δίωξη του ηλεκτρονικού εγκλήματος. Στη συνέχεια θα γίνει περιγραφή και παρουσίαση των πιο σημαντικών μεθοδολογιών και εργαλείων, τα οποία παρέχονται μέσω της επιστήμης με στόχο να αξιολογηθούν οι σημαντικότερες εκ αυτών και να χρησιμοποιηθούν σε πρακτικό επίπεδο.
Ιδιαίτερο βάρος θα δοθεί στα Δικανικές Υπηρεσίες Ιστού (Web Services Forensics-FWS) τα οποία αποτελούν ένα τομέα της «Δικανικής Πληροφορικής» με ιδιαίτερο επιστημονικό ενδιαφέρον. Τέλος, θα γίνει προσομοίωση εξεύρεσης ψηφιακών πειστηρίων κάνοντας χρήση της καλύτερης μεθοδολογίας μέσω ενός εικονικού περιβάλλοντος (testing environments) που θα δημιουργηθεί με χρήση εικονικών εργαστηριών (Virtual Lab) καθώς και η χρήση των κατάλληλων εργαλείων που θα παρουσιαστούν στις παρακάτω ενότητες καθώς και η αξιολόγηση των διάφορων αποτελεσμάτων.

Abstract

This thesis is a theoretical description of the fundamental principles of "Forensic Computer 'and an experimental presentation of technical components of this science. There will be a reference to the definitions and the concepts which belonging to the "Forensic Computing. A description will be given of the specified legal framework through which the data provided to judicial authorities as having the aim of prosecuting cybercrime. Subsequently a presentation of the most important methodologies and tools, which are provided by science in order to assess the most important of these and used in practice.
Particular emphasis will be given to Forensic Web Services (FWS) which constitute a field of "Forensic Computer" with special scientific interest. Finally, a simulation Forensic finding by using the best methodology through a virtual environment (Virtual Labs) and the use of the appropriate tools that will be presented in the following sections and the evaluation of the different results.

Περιεχόμενα

1 Εισαγωγή

Η είσοδος των υπολογιστικών συστημάτων σε όλους τους τομείς της σύγχρονης ζωής όπως η εκπαίδευση, ο επιστημονικός τομέας, ο δημόσιος τομέας, οι ιδιωτικές επιχειρήσεις, αποτέλεσαν χρήσιμο εργαλείο για την ανάπτυξη της αποδοτικότητας των παραπάνω τομέων με την δημιουργία αυτοματισμών που διευκόλυναν στην επίλυση πολύπλοκων προβλημάτων. Ηλεκτρονικές συναλλαγές μεταξύ φυσικών προσώπων ή και εταιρειών, απομακρυσμένη επικοινωνία μέσω βιντεοκλήσεων ή μέσω ηλεκτρονικού ταχυδρομείου, ηλεκτρονική ανταλλαγή διαφόρων τύπων αρχείων, κοινωνική δικτύωση, ψηφιακή ενημέρωση αποτελούν μερικά παραδείγματα όπου η ψηφιακή εποχή μας διευκολύνει την καθημερινότητα, παρέχοντας τα απαραίτητα τεχνολογικά εργαλεία.

Η χρήση των ψηφιακών μέσων δεν επέφερε μόνο θετικές εξελίξεις στην καθημερινότητα. Η εισαγωγή των υπολογιστών δημιούργησε πρόσφορο έδαφος για κακόβουλες ενέργειες και παράνομες δραστηριότητες χρησιμοποιώντας τα υπολογιστικά συστήματα ως εγκληματικά εργαλεία. Σύμφωνα με έρευνες[1] (1), πάνω από τριάντα ένα χιλιάδες άτομα, σε εικοσιτέσσερις χώρες παγκοσμίως, πέφτουν θύματα του ηλεκτρονικού εγκλήματος κατά την διάρκεια ενός έτους. Ακόμα, οι έρευνες δείχνουν ότι το 69% των ενηλίκων έχει πέσει θύμα ηλεκτρονικής απάτης. Αξίζει να σημειωθεί ότι το οικονομικό κόστος που δημιουργείται λόγω του ηλεκτρονικού εγκλήματος ανέρχεται στο άθροισμα του στο ποσό των 117 εκατομμυρίων ευρώ. Είναι αυταπόδεικτο, ότι το ηλεκτρονικό έγκλημα μπορεί να προκαλέσει μεγάλες οικονομικές ζημιές, διαρροή προσωπικών πληροφοριών και ευαίσθητων δεδομένων, πλαστογραφία, σε επιχειρήσεις, κυβερνητικούς οργανισμούς , αλλά και σε φυσικά πρόσωπα.

Με την τεχνολογική πρόοδο και καθιστώντας την χρήση των υπολογιστικών συστημάτων αναντικατάστατη στην καθημερινή μας ζωή, είχε σαν αποτέλεσμα πολλοί επίβουλοι χρήστες να έχουν αποκτήσει άριστες τεχνικές δεξιότητες και να διαπράττουν κάθε μορφής ηλεκτρονικά εγκλήματα παραβαίνοντας τους ισχύοντες νόμους. Διάφοροι οργανισμοί, είτε δημόσιοι είτε ιδιωτικοί, δέχονται δεκάδες επιθέσεις καθημερινά. Αξίζει να σημειωθεί ότι οι επιθέσεις που δέχεται ένας οργανισμός στα πληροφοριακά του συστήματα δεν προέρχονται μόνο από εξωτερικούς χρήστες. Πολλές φορές χρήστες από το εσωτερικό ενός φορέα προκαλούν δολιοφθορές στο εσωτερικό μιας εταιρείας, δημιουργώντας κενά ασφαλείας ή κλέβοντας «ευαίσθητα» δεδομένα που μπορούν να προκαλέσουν μεγάλες οικονομικές ζημιές σε ένα οργανισμό.

Συχνό φαινόμενο αποτελεί η καταστροφή δεδομένων ή η δημιουργία κενών ασφαλείας από χρήστες που κάνουν κακή διαχείριση των υπολογιστικών συστημάτων (misuse). Για να αποφευχθούν όλοι αυτοί οι κίνδυνοι θα πρέπει ο υπεύθυνος ασφαλείας του Πληροφοριακού Συστήματος ενός οργανισμού να λάβει όλα τα μέτρα που χρειάζονται χρησιμοποιώντας όλα τα απαραίτητα τεχνολογικά εργαλεία που απαιτούνται και τις κατάλληλες μεθοδολογίες, έτσι ώστε να διατηρεί ακέραια και με ασφάλεια τα δεδομένα ενός οργανισμού για την αντιμετώπιση τέτοιων κινδύνων.

Στην περίπτωση που ένας οργανισμός πέσει θύμα ηλεκτρονικού εγκλήματος, οι διωκτικές αρχές αναθέτουν σε ειδικούς ασφαλείας να συλλέξουν δεδομένα για τον εντοπισμό της επίθεσης. Οι ειδικοί ασφαλείας των Διωκτικών Αρχών σε συνεργασία με τους υπεύθυνους ασφαλείας του οργανισμού, συλλέγουν και αναλύουν όλα τα απαραίτητα αποδεικτικά στοιχεία κάνοντας χρήση τεχνολογικών εργαλείων που παρέχει η επιστήμη της Δικανικής Πληροφορικής. Τέλος, τα

[1] Έρευνα του Norton Cyber Crime Report. http://us.norton.com/cybercrimereport/

αποτελέσματα της ανάλυσης των δεδομένων της επίθεσης μπορούν να χρησιμοποιηθούν στο δικαστήριο, στα πλαίσια πάντα του εκάστοτε Νομοθετικού Πλαισίου.

2 Εννοιολογικοί ορισμοί

Τα σύγχρονα πολυσύνθετα Πληροφοριακά Συστήματα και δίκτυα διαφόρων οργανισμών, αποτελούν στόχο κακόβουλων ατόμων με στόχο την υποκλοπή, καταστροφή ή αλλοίωση των δεδομένων. Σε αρκετές περιπτώσεις, κακόβουλη πράξη μπορεί να θεωρηθεί όχι μόνο μια επίθεση που προέρχεται από το Διαδίκτυο αλλά και μια εσκεμμένη επίθεση από το εσωτερικό δίκτυο ενός οργανισμού ή ακόμα λανθασμένη διαχείριση των πληροφοριακών πόρων (misuse).

Όλοι οι παραπάνω λόγοι εισήγαγαν την έννοια της ασφάλειας στην επιστήμη της πληροφορικής. Η ανάγκη για ασφάλεια όλων των πληροφοριακών πόρων όπως το δίκτυο, τα αρχεία, η υποδομή (Infrastructure), το λογισμικό και γενικότερα όλα τα πληροφοριακά μέσα που αποτελούν βασικό κορμό της παραγωγής ενός οργανισμού, καθιστά αναγκαία συνθήκη την χρήση προηγμένων τεχνολογικών μέσων, διαδικασιών και εργαλείων που θα αποτρέψουν τέτοιου είδους εγκληματικές ενέργειες.

Στην παρούσα εργασία θα παρουσιαστούν και θα προταθούν κατάλληλες μεθοδολογίες, οι οποίες θα ακολουθούν ένα συγκεκριμένο πλαίσιο διαδικασιών σε ένα συμβάν επίθεσης καθώς επίσης και εκείνα τεχνολογικά εργαλεία που θα βοηθήσουν στην πρόληψη αλλά και αποτροπή εγκληματικών επιθέσεων. Ο συνδυασμός των μεθοδολογιών και η χρήση των κατάλληλων πληροφοριακών εργαλείων της Δικανικής Πληροφορικής, θα επιτρέψουν στους ειδικούς εγκληματολόγους να παρουσιάσουν στις διάφορες Δικαστικές Αρχές και βάση του ισχύοντος Νομοθετικού Πλαισίου, τα αποδεικτικά στοιχεία που θα επιτρέψουν την δίωξη ενός Ηλεκτρονικού Εγκλήματος.

Ιδιαίτερη έμφαση θα δοθεί στην ασφάλεια των Υπηρεσιών Ιστού (Web Services). Σαν Υπηρεσία Ιστού ορίζεται μια μέθοδος επικοινωνίας μεταξύ δύο ή περισσοτέρων ηλεκτρονικών συσκευών (συνήθως εξυπηρετητών ιστού), μέσω ενός δικτύου υπολογιστών[2]. Τις υπηρεσίες ιστού, με την ραγδαία ανάπτυξη του διαδικτύου, τις συναντάμε από μικρές διαδικτυακές εμπορικές σελίδες (π.χ. e-shop), σε Δημόσιους οργανισμούς καθώς επίσης και σε πολυεθνικές επιχειρήσεις. Οι υπηρεσίες ιστού διευκολύνουν και επιταχύνουν τις διαδικασίες ενός οργανισμού, Δημόσιου ή Ιδιωτικού. Για παράδειγμα μέσω του διαδικτύου ένας χρήστης μπορεί να κάνει κράτηση ενός αεροπορικού εισιτηρίου καταχωρώντας τα προσωπικά του στοιχεία σε μια φόρμα εγγραφής, στη συνέχεια μια άλλη υπηρεσία αναλαμβάνει την συναλλαγή για την πληρωμή και την εξακρίβωση των στοιχείων του πελάτη με την αντίστοιχη υπηρεσία ιστού της επιθυμητής Τράπεζας. Τέλος, μια άλλη υπηρεσία αναλαμβάνει να ενημερώσει τη βάση της αεροπορικής εταιρείας για την επιτυχή κράτηση του εισιτηρίου. Η πολυπλοκότητα των υπηρεσιών ιστού μπορεί να ποικίλει ανάλογα την συναλλαγή, στο παραπάνω παράδειγμα πολλές συναλλαγές μεταξύ των υπηρεσιών απαιτούν μεθόδους κρυπτογράφησης καθώς και άλλων μέτρων ασφαλείας ακόμα και στο κομμάτι του τεχνολογικού εξοπλισμού ενός οργανισμού. Σε μια τέτοια συναλλαγή υπάρχει πάντα ο κίνδυνος κάποιος να υποκλέψει τα στοιχεία ενός χρήστη (man in the middle) ή ακόμα να υποκλέψει ευαίσθητα δεδομένα πελατών όπως αριθμούς πιστωτικής κάρτας, αριθμούς λογαριασμών κτλ. Μια τέτοια παράνομη διείσδυση μπορεί να προκαλέσει οικονομικές απώλειες σε μια εταιρεία είτε με άμεσο τρόπο, καταστροφή δεδομένων, πλήγμα στην αξιοπιστία της εταιρείας, είτε έμμεσα αδυναμία να λειτουργήσει αποδοτικά ο οργανισμός- παρεμπόδιση επιχειρησιακής συνέχειας.

[2] Ορισμός Υπηρεσιών Ιστού – Web Services : http://en.wikipedia.org/wiki/Web_service .

Όλα τα ανωτέρω υποχρεώνουν τον υπεύθυνο ασφαλείας των Πληροφοριακών Συστημάτων του οργανισμού να λάβει όλα αυτά τα μέτρα προστασίας που θα του επιτρέπουν να ελέγχει και να διαμορφώνει το πληροφοριακό περιβάλλον με ασφαλή μέτρα και αυτοματοποιημένες μεθόδους με τις οποίες θα μπορεί να διαχειριστεί ευκολότερα ένα γεγονός κρίσης και θα διευκολύνει την συλλογή πειστηρίων από τους ειδικούς Εγκληματολογικούς Ερευνητές. Μέσω των διαδικασιών που περιγράφονται στην ενότητα 2.1.1 οι Εγκληματολόγοι των ηλεκτρονικών επιθέσεων θα συλλέξουν τα κατάλληλα δεδομένα και θα τα παρουσιάσουν στις Δικαστικές Αρχές. Τέλος, με βάση το ισχύον Νομοθετικό πλαίσιο και τα αποδεικτά στοιχεία που έχουν συλλεχθεί, το Δικαστήριο καταλήγει σε κάποιο πόρισμα.

Συνεπώς, αναμφισβήτητα στη σύγχρονη κοινωνία θα πρέπει να υπάρχουν αυτοματοποιημένες μέθοδοι και όλα τα τεχνολογικά μέσα τα οποία θα επιτρέπουν την εύκολη διαχείριση, παρακολούθηση και ασφάλεια των πληροφοριακών συστημάτων.

2.1 Ορισμός «Δικανική Πληροφορική»

Η Δικανική εγκληματολογία είναι η διαδικασία χρήσης επιστημονικής γνώσης για την συλλογή, ανάλυση και παρουσίαση αποδεικτικών στοιχείων στα Δικαστήρια. Οι Δικανικές διαδικασίες στοχεύουν πρωτίστως στην ανάκτηση και την ανάλυση των «κρυφών» δεδομένων. Τα «κρυφά» δεδομένα μπορούν να πάρουν διάφορες μορφές όπως δαχτυλικά αποτυπώματα σε ένα παράθυρο, αποδεικτικά στοιχεία από DNA ή ακόμα και αρχεία από ένα σκληρό δίσκο.

Σαν Δικανική πληροφορική (ή Δικανική Υπολογιστική), ορίζουμε *την πλήρη εφαρμογή των διαδικασιών που συνδυάζουν στοιχεία του νόμου και της επιστήμης των υπολογιστών έτσι ώστε να συλλεχτούν και να αναλυθούν τα δεδομένα από τα συστήματα ηλεκτρονικών υπολογιστών, υπηρεσιών ιστού, δεδομένα δικτύου, ηλεκτρονικών επικοινωνιών και μέσων αποθήκευσης με τρόπο που θα είναι αποδεκτός ως πειστήριο σε ένα δικαστήριο στηριζόμενο στο ισχύον νομοθετικό πλαίσιο ενός κράτους* (2).

Η αλλαγή των κοινωνικών ρυθμών και η τεχνολογική πρόοδος κάνει αναγκαία την χρήση κάθε ηλεκτρονικού μέσου για την επικοινωνία και ανταλλαγή πληροφοριών μεταξύ των οργανισμών και των σύγχρονων επιχειρήσεων. Σαν συνέπεια της τεχνολογικής προόδου εμφανίστηκε το ηλεκτρονικό έγκλημα. Κακόβουλοι χρήστες με τεχνολογικές δεξιότητες επιτίθενται σε διάφορα πληροφοριακά συστήματα για λόγους υποκλοπής προσωπικών δεδομένων, εκβιασμό, υπεξαιρέσεις, βιομηχανική κατασκοπεία, κλοπής χρημάτων από τραπεζικούς λογαριασμούς, «χτύπημα» στην αξιοπιστία ενός οργανισμού ακόμα και για λόγους επίδειξης των ικανοτήτων τους (Grey Hat).Η εγκληματική αυτή παρείσφρηση στις τεχνολογικές πλατφόρμες ανάγκασε πολλές επιχειρήσεις να προσλαμβάνουν ειδικούς της Δικανικής πληροφορικής για να συλλέξουν αποδεικτικά στοιχεία σε περιπτώσεις εκβιασμών, διαρροών ευαίσθητων πληροφοριών ή παράνομης πρόσβασης.

Η Δικανική πληροφορική μοιάζει να είναι ολοένα και περισσότερο αναγκαία έτσι ώστε να διασφαλίσει τη συνολική ακεραιότητα και την ικανότητα επιβίωσης της πληροφοριακής υποδομής ενός οργανισμού. Παρόλο που έγιναν πολλές προσπάθειες για να αναπτυχθεί ένα μοντέλο Δικανικών διαδικασιών κανένα έως σήμερα δεν έχει γίνει κοινά αποδεκτό. Αυτό οφείλεται κυρίως ότι πολλά μοντέλα είχαν σχεδιαστεί για να έχουν εφαρμογή σε ένα συγκεκριμένο περιβάλλον, όπως για παράδειγμα συγκεκριμένη νομοθεσία και επιβολή του νόμου σε ένα κράτος. Η αδυναμία εφαρμογής ενός κοινού πλαισίου οδήγησε στην ανάπτυξη επιστημονικών μεθοδολογιών οι οποίες βασίζονται στις βασικές αρχές ασφάλειας των πληροφοριακών συστημάτων και των

σύγχρονων τεχνολογικών εξελίξεων. Μερικές αξιόλογες εξ αυτών παρουσιάζονται στην 3η ενότητα.

Η Δικανική Υπολογιστική έχει της ρίζες της στην Δικανική εγκληματολογία. Στην περίπτωση της Δικανικής εγκληματολογίας και για παράδειγμα στην περίπτωση μιας δολοφονίας ο ειδικός εγκληματολόγος θα πρέπει να συλλέξει πειστήρια από την σκηνή του εγκλήματος κάνοντας αυτοψία, στην συνέχεια θα πρέπει να ανακατασκευάσει το συμβάν και να αναλύσει τα δεδομένα. Τεχνικές βαλλιστικής εξέτασης και ανάλυσης DNA, είναι από τις πιο κοινές σε τέτοιου είδους υποθέσεις. Τέλος αφού συλλεχθούν όλα τα απαραίτητα αποδεικτικά στοιχεία, θα πρέπει να συνταχτεί έκθεση από τον ειδικό ερευνητή που θα παρουσιάζει όλα αυτά τα δεδομένα που έχουν συλλεχθεί και θα υποδεικνύουν τον υπεύθυνο της εγκληματικής πράξης που θα οδηγήσουν τους υπαίτιους σε δίκη και θα εφαρμοστούν οι ισχύοντες νόμοι.

Αποδεικνύεται ότι η σωστή εφαρμογή των μεθοδολογιών της Δικανικής πληροφορικής μπορεί να επιφέρει πολλά οφέλη και να μειώσει τον κίνδυνο από το κόστος που θα φέρει μια επικείμενη επίθεση σε ένα οργανισμό, όπως για παράδειγμα διαρροή ευαίσθητων πληροφοριών, χρηματικό κόστος, ανάκτηση χαμένων ή αλλοιωμένων δεδομένων. Τέλος, παρέχει την ασφάλεια ότι θα καλύψει με τα εργαλεία και τις διαδικασίες τυχόν κενά ασφαλείας ενός πληροφοριακού συστήματος και θα παρέχει όλη αυτή την πληροφορία και τα πειστήρια που θα χρειαστούν σε μια Δικαστική διαμάχη ενάντια στους υπαίτιους μια ηλεκτρονικής επίθεσης.

2.1.1 Διαδικασίες «Δικανικής Πληροφορικής»

Κατά την εφαρμογή των Δικανικών μεθοδολογιών ακολουθούνται οι παρακάτω διαδικασίες , οι οποίες αποτελούν και αντίμετρα για την προστασία από συμβάντα επιθέσεων.

1. Πρόληψη κατά των κακόβουλων πράξεων. Μέτρα όπως το τείχος προστασίας (firewall), ενδιάμεσοι εξυπηρετητές (proxies), ασφαλίζουν και αποτρέπουν από ένα πληροφοριακό περιβάλλον μη εξουσιοδοτημένες εισόδους.
2. Η ανίχνευση «ύποπτων» κινήσεων σε ένα πληροφοριακό δίκτυο. Με την χρήση Συστημάτων Ανίχνευσης Εισβολών (Intrusion Detection Systems-IDS), έχουν στόχο την ανίχνευση εισβολέων ή μη αναμενόμενων κινήσεων των πακέτων του δικτύου.
3. Η συλλογή ψηφιακών αποδείξεων. Περιλαμβάνονται όλες μέθοδοι για έτσι ώστε να δημιουργηθεί πιστό αντίγραφο των πρωτότυπων ψηφιακών αποδείξεων, έτσι ώστε να καταγραφεί το συμβάν της επίθεσης.
4. Διατήρηση των πειστηρίων. Τα αποδεικτικά στοιχεία τα οποία έχουν εξαχθεί από αποδεκτές πρακτικές μεθόδους, θα πρέπει να απομονωθούν και να προστατευτούν έτσι ώστε να παραμείνουν αναλλοίωτα στην αρχική τους μορφή.
5. Ανάλυση των ψηφιακών αποδείξεων. Θα πρέπει να επιλεχθούν τα ποιο σημαντικά δεδομένα που έχουν συλλεχθεί, μετά από ένα συμβάν επίθεσης, έτσι ώστε να εξαχθούν πιο ασφαλή συμπεράσματα τα οποία θα ευσταθούν σε μια Δικαστική αίθουσα.
6. Ανακατασκευή της επίθεσης. Εφόσον έχουν επιλεχθεί τα σημαντικότερα αποδεικτικά στοιχεία, γίνεται προσπάθεια ανακατασκευής και αναπαραγωγής του συμβάντος της επίθεσης, έτσι ώστε να εντοπισθεί η πηγή της επίθεσης καθώς και τα σημεία του πληροφοριακού περιβάλλοντος έχουν προσβληθεί.
7. Αποκατάσταση του πληροφοριακού περιβάλλοντος. Θα πρέπει να έχουν ληφθεί τα μέτρα εκείνα που θα επιτρέψουν την ελαχιστοποίηση του χρόνου αποκατάστασης του παραγωγικού πληροφοριακού περιβάλλοντος.
8. Παρουσίαση πειστηρίων. Στη τελική φάση των διαδικασιών, θα πρέπει να γίνει καταγραφή και παρουσίαση των αποδεικτικών στοιχείων. Τα δεδομένα θα πρέπει να

είναι περιεκτικά, δομημένα με σαφήνεια και τα συμπεράσματα που έχουν εξαχθεί κατόπιν της έρευνας θα πρέπει να ευσταθούν στην περίπτωσή μιας δίκης.

2.1.2 Ηλεκτρονικό έγκλημα – Ψηφιακοί κίνδυνοι

Οι ολοένα και αυξανόμενοι κίνδυνοι από τα εγκλήματα που διαπράττονται σε βάρος των υπολογιστικών συστημάτων και συγκεκριμένα στις πληροφορίες που διατηρούν αυτά, έχουν αρχίσει να «τραβάνε» την προσοχή των διαφόρων κρατών. Η υφιστάμενη νομοθεσία στις περισσότερες χώρες σε όλο τον κόσμο, είναι πιθανό να είναι μην είναι εφαρμόσιμη εναντίον τέτοιων εγκλημάτων (21). Αυτή η έλλειψη νομικής προστασίας σημαίνει ότι οι επιχειρήσεις και οι κυβερνητικοί οργανισμοί πρέπει να βασίζονται αποκλειστικά σε τεχνικά μέτρα προστασίας που θα πρέπει να λάβουνε από μόνοι τους έτσι ώστε να αποτρέψουν ηλεκτρονικές επιθέσεις υποκλοπής ευαίσθητων δεδομένων, άρνησης πρόσβασής ή ακόμα και αλλοίωση πληροφοριών.

Η λήψη μέτρων ασφαλείας και η αυτό-προστασία, παρόλο που κρίνεται απαραίτητη δεν εξαλείφει τους κινδύνους που εντοπίζονται στον κυβερνοχώρο. Σε αυτή την περίπτωση θα πρέπει να επέμβει το κράτος με τις νομοθεσίες που θα είναι ικανές να αντιμετωπίσουν τέτοιου είδους σενάρια επιθέσεών. Δεδομένου ότι η εγκληματικότητα στον κυβερνοχώρο παραβιάζει όλο και περισσότερο τα εθνικά σύνορα, πολλά κράτη διατρέχουν τον κίνδυνο να γίνουν λιγότερο ανταγωνιστικά στο παγκόσμιο οικονομικό πλαίσιο. Η χαμηλή ασφάλεια πληροφοριών μειώνει την ανταγωνιστικότητα των Εθνών. Σε αυτή την περίπτωση οι εκάστοτε κυβερνήσεις θα πρέπει να εξετάσουν τις ισχύουσες νομοθεσίες και να διαπιστώσουν κατά πόσον είναι επαρκείς για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Όπου υπάρχουν κενά, οι κυβερνήσεις θα πρέπει να βασιστούν στις βέλτιστες πρακτικές που έχουν εφαρμοστεί από άλλες χώρες πιο «ώριμες» στο τομέα αυτό και να συνεργαστούν στενά με τη βιομηχανία της χώρας για να θεσπιστεί η νομική προστασία έναντι αυτών των νέων μορφών εγκλημάτων. Οι κυβερνήσεις, η βιομηχανία και οι διάφοροι δημόσιοι οργανισμοί θα πρέπει να εφαρμόσουν τους νόμους που θα θεσπιστούν αποτελεσματικά κατά των εγκληματιών του διαδικτύου.

Η αποτελεσματική επιβολή του νόμου περιπλέκεται από τη διακρατική φύση του κυβερνοχώρου. Οι μηχανισμοί συνεργασίας πέρα από τα εθνικά σύνορα καθιστούν την δίωξη ηλεκτρονικών εγκλημάτων πολύ αργή και πολύπλοκη. Οι διαδικτυακοί εγκληματίες είναι σε θέση να εφαρμόζουν τεχνικές επίθεσης από ένα υπολογιστή που μπορεί να βρίσκεται οπουδήποτε ανά τον κόσμο, περνώντας διαμέσου υπολογιστικών δικτύων πολλών χωρών και ειδικά από τα δίκτυα κρατών που παρουσιάζουν ελλείψεις στη νομοθεσία τους, καθιστώντας δύσκολη την σύλληψη τους και αποκρύπτοντας αποτελεσματικά την ταυτότητα τους.

Στον παρακάτω πίνακα (3) παρουσιάζονται στοιχεία χωρών που οι νόμοι έχουν ενημερωθεί σε κάθε μια από αυτές με πλήρη, ουσιαστικά ή μερικώς ενημερωμένους νόμους.

Countries with Updated Laws										
Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	✔	✔	✔	✔		✔			✔	✔
Brazil		✔			✔	✔		✔		
Canada	✔	✔	✔	✔	✔	✔	✔			✔
Chile	✔	✔	✔	✔	✔					
China		✔		✔			✔			
Czech Republic		✔	✔		✔	✔				✔
Denmark		✔		✔						✔
Estonia		✔	✔	✔	✔	✔	✔	✔		✔
India		✔	✔	✔	✔	✔	✔	✔		✔
Japan	✔	✔	✔	✔	✔	✔		✔	✔	✔
Malaysia		✔				✔		✔		✔
Mauritius	✔	✔		✔	✔	✔	✔	✔	✔	
Peru	✔	✔	✔	✔	✔	✔				✔
Philippines	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Poland		✔	✔	✔				✔		
Spain	✔	✔	✔					✔		✔
Turkey		✔	✔	✔	✔		✔	✔	✔	✔
United Kingdom		✔		✔	✔	✔		✔		
United States	✔	✔	✔	✔	✔	✔	✔	✔		✔

Εικόνα 1. Πίνακας κρατών που ενημέρωσαν τις νομοθεσίες τους οι οποίες σχετίζονται με ηλεκτρονικές απειλές.

Τα Ευρωπαϊκά κράτη συμπεριλαμβανομένης και της Ελλάδας, για να αντιμετωπίσουν τον ηλεκτρονικό έγκλημα συμφωνήσαν σε μια κοινή στρατηγική και υπέγραψαν την μέχρι τώρα ισχύουσα Συνθήκη στο Συνέδριο της Βουδαπέστης το 2001 (Convention on Cyber Crime). Στην ενότητα 2.1.6 παρουσιάζεται αναλυτικά η νομοθεσία του Ελληνικού κράτους ενάντια στους ηλεκτρονικούς κινδύνους.

Σύμφωνα με την έρευνα της LLC, McConnell International, «Cyber Crime... and Punishment?» (3), κατατάσσει τα ηλεκτρονικά εγκλήματα που διαπράττονται στο διαδίκτυο στις εξής κατηγορίες: τροποποίηση και κλοπή δεδομένων, πλαστογραφία και απάτη, υπόθαλψη αδικημάτων, μη εξουσιοδοτημένη πρόσβαση, διασπορά κακόβουλων ιών μέσω διαδικτύου, παρεμπόδιση κυβερνο-κυκλοφορίας, εισβολή και επίθεση σε ιδιωτικό δίκτυο.

Στην Ελλάδα συγκεκριμένα, σύμφωνα με το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ (4), έχουν αντιμετωπιστεί και εξιχνιαστεί οι εξής κατηγορίες κυβερνοεπιθέσεων:

- Κλοπή πιστωτικών καρτών.

- Διαδικτυακές απάτες.
- Παιδική πορνογραφία.
- Διακίνηση ναρκωτικών.
- Εγκλήματα σε δωμάτια συζητήσεων (chat rooms), όπως εκβιασμούς, παραπλανήσεις.
- Διακίνηση πειρατικού λογισμικού.
- Περιπτώσεις επιθέσεων Hacking.

Τέλος, ενδιαφέρον παρουσιάζει η έρευνα της εταιρίας Symantec Norton Security το 2013 (5), όπου αναφέρει ότι ο υψηλότερος αριθμός εγκληματικότητας στον κυβερνοχώρο, σε δείγμα 24 χωρών, παρουσιάζεται στη Ρωσία με 85% ακολουθεί η Κίνα με 75% και τέλος στη Νότιο Αφρική με ποσοστό θυμάτων 73%. Ακόμα είναι πιο πιθανό να πέσουν θύματα απάτης άντρες σε ποσοστό 64% έναντι του 58% των γυναικών και εξ αυτών:

1. Το 63% είναι χρήστες κινητών τηλεφώνων.
2. Το 68% χρησιμοποιούσαν δημόσια και μη ασφαλή ασύρματα δίκτυα.
3. Το 63% έκαναν χρήση ιστοσελίδων κοινωνικής δικτύωσης.
4. Το 68% έπεσαν θύματα ηλεκτρονικών αγορών.
5. Τέλος το 65% αφορά παιδιά ηλικίας 8-17 ετών που δεν είχαν την επιμέλεια των γονέων όταν έκαναν χρήση του διαδικτύου.

2.1.3 Ψηφιακά Πειστήρια και Δεδομένα

Σαν ψηφιακά πειστήρια ορίζουμε οποιαδήποτε πληροφορία που έχει αποθηκευτεί σε ένα ψηφιακό μέσο ή έχει μεταδοθεί μέσου αυτού και έχει αποδεικτική αξία σε μια Δικαστική αίθουσα. Η επιστήμη των ψηφιακών πειστηρίων αναλαμβάνει να αναλύσει όλα τα ηλεκτρονικά δεδομένα να ανακτήσει τις ψηφιακές πληροφορίες που μπορεί να σχετίζονται με μια κακόβουλη ενέργεια, να αναλύσει τα δεδομένα αυτά και να καταγράψει τα σχετικά ευρήματα σε μια έκθεση για δικαστική χρήση. Η αναζήτηση των ψηφιακών πειστηρίων γίνεται από ειδικούς επιστήμονες οι οποίοι θα μπορούν να διαλευκάνουν για το ποια δεδομένα έχουν τροποποιηθεί ή καταστραφεί. Τα πειστήρια που θα συλλεχτούν θα πρέπει να είναι αυθεντικά, αξιόπιστα και να πληρούν όλες τις προϋποθέσεις σύμφωνα με το εθιμικό δίκαιο και τους κανόνες δικαίου.

Ψηφιακά δεδομένα μπορούν να αποθηκευτούν σε σκληρούς δίσκους και συνήθως όταν αναφερόμαστε σε κάποιον οργανισμό ή επιχείρηση σε file servers και μεγάλα storage συστήματα. Ακόμα μπορούν να περιέχονται σε μέσα αποθήκευσης όπως cd-rom, usb flash μνήμες, μαγνητικές ταινίες (backup disks), εξωτερικούς δίσκους και ακόμα σε volatile μνήμες (RAM).

Οι ειδικοί εγκληματολόγοι, στα μέσα αποθήκευσης που παρουσιάστηκαν στην προηγούμενη παράγραφο, θα αναζητήσουν αποδείξεις σε ψηφιακά αρχεία που μπορούν να βρεθούν:

- Κρυπτογραφημένα με διάφορους αλγόριθμους κρυπτογράφησης (Caesar cipher, Vigenere cipher). Αξίζει να αναφερθεί η μέθοδος της στενογραφίας (steganography) κατά την οποία μπορούν να κρυπτογραφηθούν δεδομένα μέσα σε ένα αρχείο εικόνας ή ένα αρχείο ήχου, αρχεία φωτογραφιών ή αρχεία που έχουν δημιουργηθεί με διάφορες μεθόδους.
- Αρχεία που δημιουργούνται από τα πληροφοριακά συστήματα και αφορούν τις συναλλαγές και το αποτύπωμα των χρηστών στις διάφορες ενέργειες τους, όπως είσοδος – έξοδος σε μια υπηρεσία, ποια αρχεία χρησιμοποίησαν και τροποποίησαν, περιήγηση στο διαδίκτυο (cookies). Σημαντικές πληροφορίες μπορούν να εξαχθούν από την ηλεκτρονική αλληλογραφία των χρηστών.

- Αρχεία που δημιουργούνται από το σύστημα και αφορούν υπηρεσίες, εφαρμογές και μεταφορά δεδομένων (κίνηση) σε ένα πληροφοριακό δίκτυο όπως τα αρχεία καταγραφής συμβάντων όπως πίνακες δρομολόγησης (Routing tables), ARP cache εγγραφές.
- Τέλος, αρχεία τα οποία έχουν αποθηκευτεί εσκεμμένα στον unallocated χώρο ενός σκληρού δίσκου, δεδομένα που έχουν διαγραφεί και αποτελούν πειστήρια, swap files[3] ή αποτυπώματα που έχουν δημιουργηθεί από την εκτέλεση ενός προγράμματος από ένα εξωτερικό δίσκο usb.

Στα σύγχρονα και πολύπλοκα πληροφοριακά συστήματα δημιουργείται η ανάγκη ύπαρξης διαδικτυακών υπηρεσιών που θα διευκολύνουν και θα επιταχύνουν τις διάφορες επιχειρησιακές ανάγκες. Ιδιαίτερο ενδιαφέρον και τεχνολογική πρόκληση παρουσιάζει η συλλογή και η ανάλυση ψηφιακών πειστηρίων σε επικοινωνίες μεταξύ των διαφόρων υπηρεσιών ιστού. Διάφορα εργαλεία όπως αρχεία καταγραφής συναλλαγών, εποπτείας της κίνησης του δικτύου μπορούν να αποδειχτούν ανεπαρκή σε πολλές περιπτώσεις για την συλλογή πειστηρίων πολλές περιπτώσεις οι επιτιθέμενοι τέτοιων ηλεκτρονικών επιθέσεων καταφέρνουν να αλλοιώσουν ή να καλύψουν τα ίχνη τους. Όπως θα παρουσιαστεί στις ενότητες που ακολουθούν οι επιχειρήσεις και οι οργανισμοί θα πρέπει να σχεδιάσουν και να υλοποιήσουν πλαίσια ασφαλείας και αντίμετρα ικανά να εντοπίσουν, να αναλύσουν και να ανασκευάσουν τέτοιου είδους επιθέσεις σε υπηρεσίες ιστού.

Σε κάθε περίπτωση οι εγκληματολόγοι της Δικανικής επιστήμης θα πρέπει να εφαρμόσουν όλες τις απαραίτητες τεχνικές και τα ειδικά εργαλεία για να απαντήσουν στα ερωτήματα για το ποιο ήταν το είδος της επίθεσης, ποιος την προκάλεσε, να κάνουν την ηλεκτρονική αναζήτηση των πειστηρίων καθώς και την επανάκτηση και την αποκατάσταση αυτών. Τέλος, θα πρέπει να τα αναλύσουν έτσι ώστε να παρουσιάσουν στις δικαστικές αρχές τη σημασία και την αξία των ευρημάτων βασιζόμενος στην επιστημονική του κατάρτιση.

2.1.4 Βασικά χαρακτηρίστηκα Ασφάλειας

Προκειμένου να προστατευτούν τα πληροφοριακά συστήματα και τα δίκτυα υπολογιστών ενός οργανισμού, σχεδιάστηκε ένα μοντέλο με σκοπό να βοηθήσει στην ασφάλεια αυτών των συστημάτων. Το μοντέλο αυτό περικλείει τρείς βασικές αρχές της εμπιστευτικότητας (confidentiality), ακεραιότητας (integrity) και της διαθεσιμότητας (availability)- γνωστό και σαν CIA.

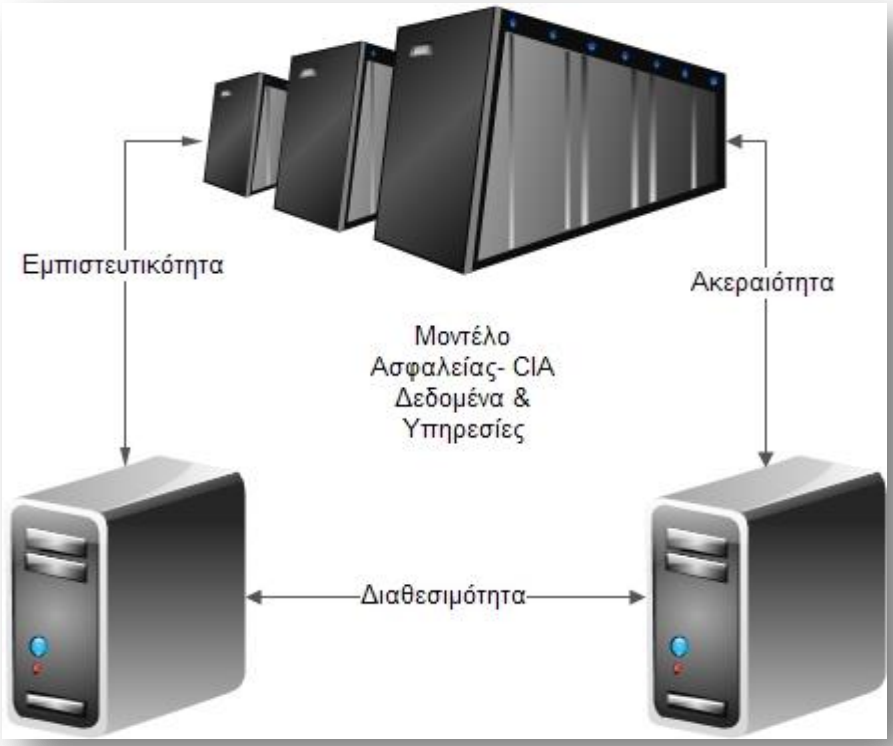
Αναλυτικότερα οι τρείς στόχοι ασφαλείας περιλαμβάνουν:

- Εμπιστευτικότητα. Έχει σχεδόν ίδια έννοια με την ιδιωτικότητα (privacy). Περιλαμβάνει όλα τα μέτρα που λαμβάνονται για τη διασφάλιση του απορρήτου ευαίσθητων πληροφοριών. Ακόμα διασφαλίζεται η αυστηρή πρόσβαση μόνο εξουσιοδοτημένων ατόμων στις εν λόγω πληροφορίες. Μερικές μέθοδοι που εξασφαλίζουν την εμπιστευτικότητα ενός πληροφοριακού συστήματος είναι η χρήση IDs και κωδικών χρηστών, οι βιομετρικοί κωδικοί όπως το δαχτυλικό αποτύπωμα και η κρυπτογράφηση δεδομένων.
- Ακεραιότητα. Περιλαμβάνει τη διατήρηση της συνοχής, την ακρίβεια και αξιοπιστία των δεδομένων σε ολόκληρο τον κύκλο ζωής του. Τα δεδομένα δεν πρέπει να αλλαχθούν κατά τη μεταφορά, και πρέπει να ληφθούν μέτρα για να διασφαλιστεί ότι τα δεδομένα δεν μπορούν να τροποποιηθούν από μη εξουσιοδοτημένα άτομα. Μερικά παραδείγματα είναι η χρήση δικαιωμάτων σε αρχεία και ο έλεγχος πρόσβασης των χρηστών. Πολλές φορές

[3] Swap files ή Page files, είναι ο χώρος σε ένα σκληρό δίσκο που χρησιμοποιείται σαν εικονική επέκταση της φυσικής μνήμης ενός υπολογιστή - RAM.

γίνεται χρήση αλγορίθμων checksum[4] (στις TCP και UDP επικοινωνίες). Αν κάποια δεδομένα έχουν αλλοιωθεί, αντίγραφα ασφαλείας θα πρέπει να είναι διαθέσιμα για την αποκατάσταση των δεδομένων σε προηγούμενη κατάσταση.

- Διαθεσιμότητα. Αποσκοπεί στη διασφάλιση ότι τα εξουσιοδοτημένα μέρη είναι σε θέση να έχουν πρόσβαση στις πληροφορίες όταν χρειάζεται. Η πληροφόρηση έχει αξία, αν οι σωστοί άνθρωποι μπορούν να έχουν πρόσβαση στους σωστούς χρόνους μόνο. Η άρνηση πρόσβασης ή διαφορετικά DDoS επίθεση (Distribute Denial of Service) στις πληροφορίες, έχει γίνει μια πολύ κοινή επίθεση στις μέρες μας. Ο πρωταρχικός στόχος των επιθέσεων DDoS είναι να εμποδίσουν τους χρήστες μιας ιστοσελίδας να έχουν πρόσβαση στους πόρους της. Τέτοιου είδους επιθέσεις μπορούν να αποδειχθούν οικονομικά ζημιογόνες για την πλειοψηφία των οργανισμών και επιχειρήσεων στις μέρες μας. Άλλοι παράγοντες που μπορεί να οδηγήσουν σε έλλειψη διαθεσιμότητας μιας υπηρεσίας είναι οι διακοπές ρεύματος ή φυσικές καταστροφές, όπως οι πλημμύρες που μπορούν να προκαλέσουν την δυσλειτουργία στην υποδομή μιας επιχείρησης.



Εικόνα 2. Μοντέλο Ασφαλείας CIA

Εκτός των προαναφερθέντων τριών βασικών αρχών ασφαλείας, υπάρχει μια πληθώρα από αρχές ασφαλείας, οι οποίες θα πρέπει να ληφθούν υπόψη σε ένα σχεδιασμό ασφάλειας πληροφοριακών συστημάτων. Εστιάζοντας στις υπηρεσίες ιστού οι έννοιες της ιδιωτικότητας (privacy) της πιστοποίησης (authentication) και του ελέγχου (auditing), είναι από τις πιο σημαντικές για προστασία και την ασφαλή μετάδοση ευαίσθητων πληροφοριών.

Οι διαδικτυακές υπηρεσίες και γενικότερα οι δυναμικές υπηρεσίες ιστού, απαιτούν κατάλληλες εγκαταστάσεις και σωστό σχεδιασμό ασφαλείας για την εξασφάλιση των απαιτήσεων ασφάλειας όλων των συμμετεχόντων. Από τη μία πλευρά οι διαδικτυακές υπηρεσίες πρέπει

[4] Το checksum είναι η καταμέτρηση του αριθμού των bits που περιλαμβάνεται σε μια μονάδα μεταφοράς, έτσι ώστε ο δέκτης μπορεί να ελέγξει για να δει αν ο ίδιος αριθμός των bits έφτασε. Εάν οι μετρήσεις ταιριάζουν, θεωρείται ότι η μετάδοση ολοκληρώθηκε.

να προστατεύονται από την καταχρηστική χρησιμοποίηση των πόρων τους και από την άλλη πλευρά, οι χρήστες των υπηρεσιών απαιτούν την προστασία της ιδιωτικής τους ζωής και των δεδομένων τους (6).

Η ιδιωτικότητα (privacy) σαν έννοια αναφέρεται στο να παραμένει απόρρητη η επικοινωνία και η ανταλλαγή πληροφοριών σε ένα πληροφοριακό δίκτυο. Συγκεκριμένα σε μια υπηρεσία ιστού ένας κακόβουλος ενδιάμεσος χρήστης να μην μπορεί να υποκλέψει καμία πληροφορία ή να αλλοιώσει την πληροφορία αυτή στο κανάλι επικοινωνίας μεταξύ του αποστολέα και του παραλήπτη του μηνύματος. Εκτός από τις κρυπτογραφικές τεχνικές, για την προστασία του απορρήτου των πληροφοριών που αφορούν το χρήστη, τα δεδομένα που χρησιμοποιούνται σε διαδικτυακές υπηρεσίες κατατάσσονται πάντοτε σύμφωνα με την εμπιστευτικότητα τους. Οι υπηρεσίες Web απαιτούν τις αντίστοιχες πιστοποιήσεις για την αντιμετώπιση των εμπιστευτικών δεδομένων.

Στην τεχνική της πιστοποίησης (authentication) και στο επίπεδο των χρηστών, η χρήση ενός «ονόματος χρήστη» (username) και ενός «κωδικού» (password) εξασφαλίζει την νόμιμη πρόσβαση αυτών σε ένα πληροφοριακό σύστημα. Πολλές φορές γίνεται χρήση κρυπτογραφικών αλγορίθμων, όπου δεν αποστέλλεται ένα απλό κείμενο (plain text). Ένα τέτοιο παράδειγμα είναι οι κρυπτογραφικοί αλγόριθμοι ροής (stream ciphers), όπου αρχικά για να κρυπτογραφηθεί το μήνυμα επιλέγεται μια γεννήτρια κλειδοροής η οποία δέχεται ως είσοδο το μυστικό κλειδί και παράγει στην έξοδό της μία ψευδοτυχαία ακολουθία bits. Βιομετρικές τεχνικές, όπως και τεχνικές κρυπτογραφίας εικόνας και ήχου εξασφαλίζουν την νόμιμη πρόσβαση διαφόρων χρηστών σε διαδικτυακές υπηρεσίες. Στο πλαίσιο των υπηρεσιών ιστού, η αρχή της πιστοποίησης (authentication), είναι η διαδικασία ταυτοποίησης των χρηστών, των εφαρμογών και των υπηρεσιών. Μπορεί να περιλαμβάνει τους τελικούς χρήστες, άλλες υπηρεσίες, διαδικασίες, ή άλλους υπολογιστές. Στην φρασεολογία της ασφάλειας, οι εξουσιοδοτημένοι χρήστες αναφέρονται ως εντολείς. Μια συνήθης τεχνική ελέγχου αυθεντικότητας μεταξύ των υπηρεσιών ενός εξυπηρετητή (server) και ενός πελάτη (client) είναι το two-way SSL. Στο two-way SSL τόσο ο πελάτης όσο και ο διακομιστής παρουσιάζουν ένα πιστοποιητικό για να αποδείξουν την ταυτότητά τους στο άλλο μέρος της υπηρεσίας. Οι ταυτότητες του πελάτη και του διακομιστή αντίστοιχα, αντιπροσωπεύονται από ψηφιακά πιστοποιητικά. Ο πελάτης και ο διακομιστής δεν χρειάζεται να εκτελούν άλλες out-of-band επικοινωνίες (όπως η χρήση καρτών ATM). Η εμπιστοσύνη μεταξύ των δύο μερών διαπιστώνεται με τα ψηφιακά πιστοποιητικά υπογεγραμμένα από κοινή αξιόπιστη αρχή πιστοποιητικών (π.χ. VeriSign, Entrust).

Ο έλεγχος (auditing), σε ένα αποτελεσματικό σύστημα καταγραφής (logging) αποτελεί το κλειδί για την μη άρνηση αναγνώρισης (non-repudiation). Τυπικά η μη άρνηση αναγνώρισης (non-repudiation) αναφέρεται στην δυνατότητα να διασφαλιστεί ότι ο συμβαλλόμενος σε μια επικοινωνία δεν μπορεί να αρνηθεί την αυθεντικότητα της υπογραφής του σε ένα έγγραφο ή για την προέλευση ενός μηνύματος που έχει αποστείλει. Σε ένα πληροφοριακό σύστημα εγγυάται ότι ένας χρήστης είναι εξουσιοδοτημένος και δεν μπορεί να του αρνηθεί η εκτέλεση μιας λειτουργίας ή μιας συναλλαγής. Για παράδειγμα, σε ένα σύστημα ηλεκτρονικού εμπορίου (e-commerce), οι μηχανισμοί μη άρνηση αναγνώρισης που απαιτούνται για να βεβαιωθεί ότι ο χρήστης δεν μπορεί να κάνει μια παραγγελία πολλών αντίγραφων ενός συγκεκριμένου προϊόντος.

Στις ενότητες που ακολουθούν θα αναλυθούν και εφαρμοσθούν πρακτικά οι βασικές αρχές ασφαλείας που περιγράφτηκαν στην συγκεκριμένη ενότητα, καθώς αποτελούν ζωτικό κομμάτι για τον σχεδιασμό και την υλοποίηση ενός πλαισίου ασφάλειας πληροφοριακών συστημάτων κατά των ηλεκτρονικών επιθέσεων.

2.1.5 Αντί-Εγκληματολογία (Anti-Forensics)

Με τον όρο Αντί – Εγκληματολογία (Anti-Forensics) εννοούμε όλα τα εργαλεία και τις τεχνικές που εμποδίζουν τα Δικανικά εργαλεία από την ορθή εγκληματολογική έρευνα. Τα Αντί-Εγκληματολογικά εργαλεία στοχεύουν:

- Στην αποφυγή ανίχνευσης.
- Την αποτροπή από διάφορα Δικανικά εργαλεία για την συλλογή χρησίμων πληροφοριών.
- Στην αύξηση του χρόνου έρευνας του Εγκληματολογικού ερευνητή, έτσι ώστε να έχει τον χρόνο ο επιτιθέμενος να καλύψει τα αποδεικτικά στοιχεία μιας επίθεσης.
- Στη εξάλειψη ή αλλοίωση τυχόν αποδεικτικών στοιχείων με στόχο να κριθούν αμφιλεγόμενα σε μια επικείμενη Δίκη.
- Στην ανακάλυψη όλων αυτών των εργαλείων που μπορούν να αποτρέψουν μια επερχόμενη επίθεση.

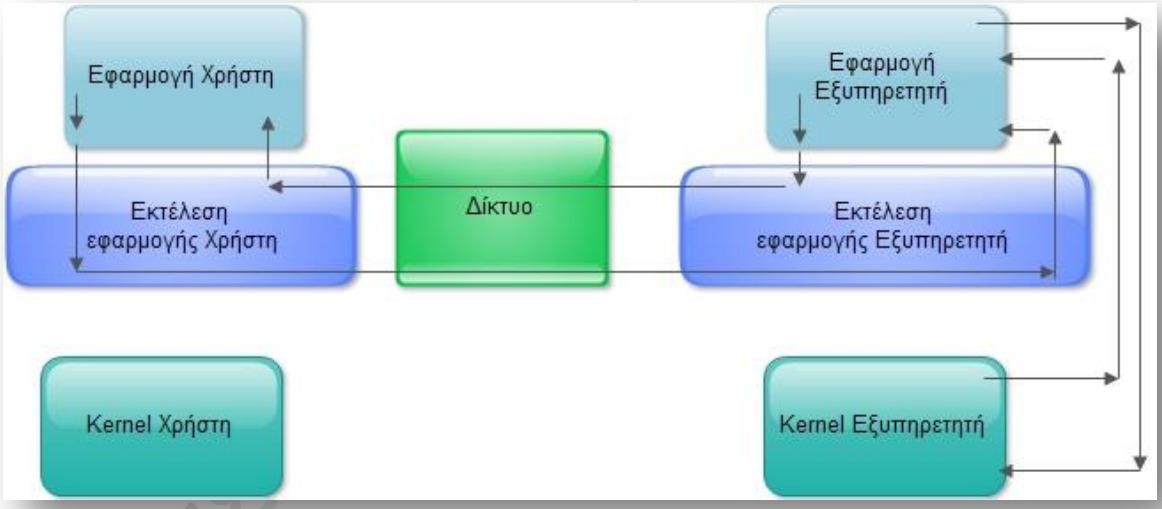
Οι Αντι-Εγκληματολογικές τεχνικές χρησιμοποιούν τις εξής μεθόδους για την επίτευξη αποτελεσματικών επιθέσεων που δεν ανιχνεύονται.

- Αποφυγή συλλογής δεδομένων που αφορούν τον επιτιθέμενο. Αποτροπή συλλογής των δεδομένων αυτών που θα μπορούν να αναλυθούν και να αποτελέσουν αποδεικτικά στοιχεία. Για παράδειγμα malware και exploitations μνήμης (memory only) δεν είναι δυνατόν να γίνουν ανιχνεύσιμα καθώς δεν εγκαθίστανται στο σκληρό δίσκο του συστήματος και επιδρούν σε πραγματικό χρόνο.
- Απόκρυψη πληροφοριών (data hiding). Όταν ένα επιτιθέμενος χρησιμοποιεί την συγκεκριμένη μέθοδο θα πρέπει να αποθηκεύσει στον δίσκο τα δεδομένα σε σημείο όπου δεν θα μπορέσει ο εγκληματολογικός αναλυτής να τα βρει. Για παράδειγμα τα Delifers toolkits τα οποία μπορούν να επικαλύψουν τα metadata δεδομένα που επιθυμεί ο επιτιθέμενος, όπως χρονοσημάνσεις (timestamps).
- Καταστροφή των δεδομένων. Ο επιτιθέμενος καταστρέφει όλα τα αποδεικτικά στοιχεία πριν κάποιος τα ανακαλύψει. Τεχνικές όπως Disk Wiping και Necrofiles χρησιμοποιούνται στην μέθοδο αυτή.
- Παραπλάνηση δεδομένων. Με τη μέθοδο αυτή παρέχονται σκοπίμως λανθασμένα δεδομένα στον εγκληματολογικό αναλυτή για διαστρέβλωση της ταυτότητας του επιτιθέμενου και του είδους της επίθεσης.
- Στεγανογραφία. Κακόβουλος κώδικας μπορεί να αποθηκευτεί σε μια εικόνα, ένα αρχείο ήχου, έτσι ώστε να είναι δύσκολο ανιχνεύσιμο.
- Κρυπτογραφημένα διαδικτυακά πρωτόκολλα. Μια διαδικτυακή κίνηση μπορεί να κρυπτογραφηθεί έτσι ώστε να αποφευχθεί η ανίχνευση της από Δικανικά εργαλεία. Σύγχρονο παράδειγμα αποτελεί η χρήση του Onion Routing που αποτελείται από πολλά επίπεδα κρυπτογράφησης. Η δρομολόγηση Onion προστατεύει και από την ανάλυση κίνησης των δεδομένων (traffic analysis). Άλλα γνωστά κρυπτογραφημένα πρωτόκολλα είναι το SSL και SSH.
- Program Packers. Η τεχνική αυτή είναι δύσκολα ανιχνεύσιμη από προγράμματα κατά των κακόβουλου κώδικα-«ιών». Η τεχνική αυτή αποτελείται από δύο εκτελέσιμα προγράμματα, το εξωτερικό εκτελέσιμο δεν ανιχνεύεται σαν κακόβουλο και ουσιαστικά, όταν αυτό εκτελεστεί, κάνει εξαγωγή του δεύτερου εκτελέσιμου που μπορεί να βλάψει

ένα σύστημα. Το κακόβουλο πρόγραμμα εξάγεται και εκτελείται στην μνήμη του συστήματος. Προγράμματα συμπίεσης είναι τα γνωστά Rootkits[5].

Τα εξελιγμένα Δικανικά εργαλεία και οι ειδικευμένοι αναλυτές καθιστούν εύκολο τον εντοπισμό δεδομένων που κάνουν χρήση των Αντί-Εγκληματολογικών μεθοδολογιών επικάλυψης και απόκρυψης δεδομένων. Τα Αντί-Εγκληματολογικά εργαλεία που μειώνουν τα αποτυπώματα μιας δραστηριότητας αποφεύγουν να αφήνουν ίχνη για περαιτέρω ανάλυση. Μερικές από τις πιο διαδεδομένες τεχνικές είναι: (i) Memory injection, (ii) Syscall Proxying, (iii) Live και Bootable images, (iv) Εικονικές Μηχανές (Virtual Machines), (v) Ανωνυμία.

Αναλυτικότερα, η τεχνική Memory Injection χρησιμοποιεί εκτελέσιμο κώδικα ο οποίος δεν είναι αποθηκευμένος σε κάποιο δίσκο αλλά εκτελείται στην μνήμη, δηλαδή ένα πρόγραμμα εκτελείται χωρίς να φορτωθεί ο εκτελέσιμος κώδικας. Τέτοιο παράδειγμα αποτελούν τα Buffer Overflow exploits. Το Syscall Proxying είναι τεχνική κατά την οποία ένα πρόγραμμα τρέχει χωρίς κώδικα. Κατά την εφαρμογή της μεθόδου του Syscall Proyxing, ένα πρόγραμμα τρέχει σε ένα υπολογιστή, τα syscalls εκτελούνται σε ένα άλλον. Το πρόγραμμα δεν είναι διαθέσιμο για ανάλυση από τους εγκληματολογικούς ερευνητές και μπορεί να δημιουργήσει μεγάλη κίνηση στο δίκτυο. Στο σχήμα που ακολουθεί περιγράφεται σχηματικά μια Syscall διαδικασία. Όπως φαίνεται και στην εικόνα που ακολουθεί ένα πρόγραμμα που θέλει να εκτελέσει κάποιος χρήστης εκτελείται τελικά στον πύρινα (kernel) ενός απομακρυσμένου εξυπηρετητή μέσω του δικτύου.



Εικόνα 3. Syscall Proxying διαδικασία.

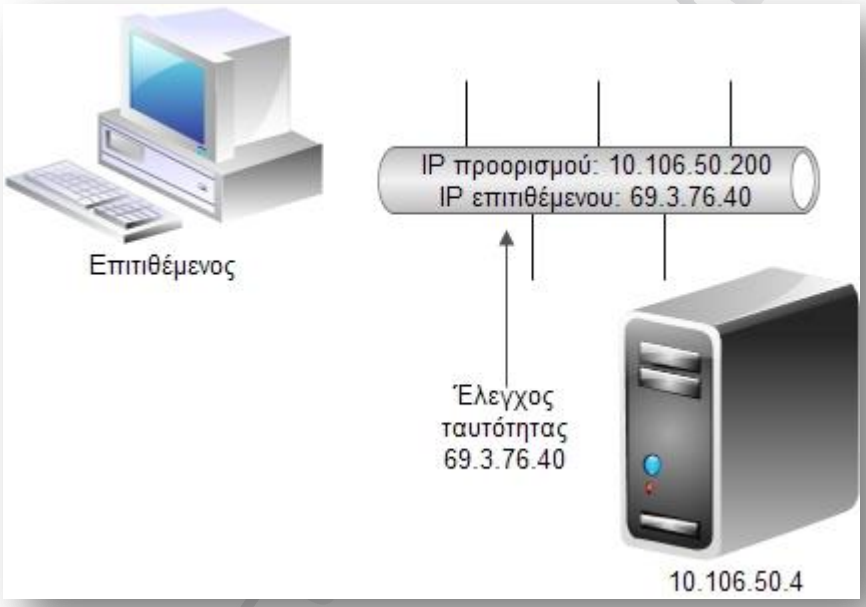
Τα Live cd's, τα Bootable USB tokens και οι Εικονικές Μηχανές, «τρέχουν» κώδικα χωρίς να αφήνουν κάποιο ίχνος. Αυτές οι προσεγγίσεις κρατάνε το σύστημα αρχείων (file system) ενός επιτιθέμενου ξεχωριστά: από την μνήμη RAM (CDs και Bootable USB tokens) και σε ένα αρχείο Εικονικής Μηχανής το οποίο μπορεί πολύ εύκολα να διαγραφεί. Τα δεδομένα ενός επιτιθέμενου μπορεί να είναι οπουδήποτε χάρη στις πολλαπλές ταυτότητες που μπορεί να έχει κάποιος, όπως

[5] Ορισμός Rootkits: http://searchmidmarketsecurity.techtarget.com/definition/rootkit .

για παράδειγμα ανώνυμοι λογαριασμοί ηλεκτρονικού ταχυδρομείου ή με την χρήση ανώνυμων IP διευθύνσεων και του πρωτοκόλλου BGP (Border Gateway Protocol).[6]

Τα Αντί-Εγκληματολογικά εργαλεία μπορούν να εντοπίσουν τα αντίστοιχα Δικανικά με τους εξής τρόπους:

- Διαφορετική ανταπόκριση των Hosts σε pings, ARPs και στην μετάδοση πακέτων με «λανθασμένη» μορφή από την αναμενόμενη.
- Οι Hosts ανταποκρίνονται σε κίνηση που δεν προοριζόταν για αυτούς, για παράδειγμα μια MAC διεύθυνση που αντιστοιχεί σε διαφορετική IP.
- Αντίστροφα DNS ερωτήματα για πακέτα που αποστέλλονται σε συγκεκριμένες IP διευθύνσεις.



Εικόνα 4. DNS queries.

Σαν αντίμετρα τα εγκληματολογικά εργαλεία έναντι των Αντί-Εγκληματολογικών θα πρέπει να χρησιμοποιούν μεθόδους εξελιγμένες όπως Keyloggers έτσι ώστε να αντιμετωπιστούν τα κρυπτογραφημένα συστήματα αρχείων και Sniffers δικτύου, έτσι ώστε να ελέγχουν και να αναλύουν συνεχώς την κίνηση.

2.1.6 Νομοθετικό πλαίσιο

Στο Διαδίκτυο «διακινούνται» πληροφορίες-δεδομένα (data) που έχουν σχέση με την προσωπική και ιδιωτική σφαίρα του ατόμου (χρήστη ή μη χρήστη του Διαδικτύου). Κάθε άτομο έχει το δικαίωμα να απαιτήσει την μη διαρροή των στοιχείων αυτών σε τρίτα «αδιάκριτα βλέμματα». Κατά συνέπεια απαιτεί τα στοιχεία αυτά να κινούνται με ασφάλεια και μυστικότητα. Η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας, αποτελούν μερικές από

[6] Το Border Gateway Protocol είναι ένα πρωτόκολλο για την ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των κόμβων , σε ένα δίκτυο αυτόνομων συστημάτων. Χρησιμοποιεί το TCP πρωτόκολλο.

τις βασικότερες αρχές του Δικαίου. Είναι ευνόητο ότι, οι θεμελιώδεις αυτές αρχές πρέπει να εφαρμόζονται και στον Κυβερνοχώρο. Ο υπερβολικός αστυνομικός έλεγχος (αστυνόμευση) του κυβερνοχώρου, δηλαδή η ευρεία διατύπωση του όρου ασφάλεια έρχεται ή ενδεχομένως να έρχεται σε αντίθεση με τις παραπάνω αρχές. Δεν μπορούμε να μιλάμε για κρατικό έλεγχο, καθότι η έννοια του Κράτους και της κρατικής κυριαρχίας είναι έννοιες άγνωστες στο Διαδίκτυο.

Είναι γνωστό ότι κάθε χρήστης του Διαδικτύου (Internet) αφήνει στον χώρο την (ηλεκτρονική) ταυτότητά του. Με κατάλληλες όμως τεχνικές παρεμβάσεις μπορεί να έχει κάποιος πρόσβαση στο διαδίκτυο ως ανώνυμος ή ακόμα και με ψευδή στοιχεία που αναφέρονται σε άλλο άτομο (18). Η παρουσίαση βέβαια με ψευδή στοιχεία μπορεί να γίνει και στο «κοινό» εγκληματικό περιβάλλον. Εκεί όμως ο εντοπισμός του δράστη είναι ευκολότερος. Μπορεί ακόμα ο χρήστης του Διαδικτύου να έχει ως στοιχείο ταυτότητας το όνομα «ανώνυμος», οπότε τυπικά φαίνεται ότι έχει όνομα. Η δυνατότητα αυτής της ανωνυμίας στο διαδίκτυο (Internet) διευκολύνει την διάπραξη παρανομιών και κάνει δύσκολο, αν όχι και αδύνατο τον εντοπισμό του δράστη. Επιπλέον, η ανωνυμία σε συνδυασμό με την ανυπαρξία ή την δυσκολία εφαρμογής των νομικών κανόνων, κάνει τους «ηλεκτρονικούς δράστες» να αισθάνονται ασφαλείς κατά τη διάπραξη των εγκλημάτων τους.

Στην Ελληνική Νομοθεσία θίγονται θέματα διαδικτύου και ειδικά θέματα που αφορούν τη συμπεριφορά των χρηστών στο παγκόσμιο ιστό. Σύμφωνα με την Ελληνική έννομη τάξη ισχύουν οι παρακάτω νομοθεσίες [11]:

- Ο Ν. 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes). Στο βαθμό λοιπόν που τα προβλεπόμενα εγκλήματα (370Β, 370Γ. 386Α) διαπράττονται και σε περιβάλλον διαδικτύου (Internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.
- Ο Ν. 2246/94 για την «οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών»
    - Ο Ν. 2774/99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, σε συνδυασμό με τον Ν. 2472/97 για την «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
    - Ο Ν. 2225/94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας.
- Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων».

Η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων. Το 2001 έγινε κατάρτιση της Διεθνούς Σύμβασης για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Σε αυτή συμμετείχε και η Ελλάδα. Σκοπός της σύμβασης είναι η προστασία της κοινωνίας από το έγκλημα στον κυβερνοχώρο, με την κατάρτιση της κατάλληλης νομοθεσίας και την επίτευξη της ανάλογης με το θέμα συνεργασίας μεταξύ των κρατών, που την υπέγραψαν.

Έχουν εκδοθεί δύο σχετικές με το θέμα συστάσεις και ειδικότερα (14):

- Η σύσταση No R(89)9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή.
- Η σύσταση No R(95)13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών.

3 Μεθοδολογίες

Σε αντίθεση με άλλες Δικανικές επιστήμες, το πεδίο της Δικανικής Πληροφορικής είναι σχετικά καινούργιο, με αποτέλεσμα να μην γίνεται εύκολα κατανοητός ο όρος Δικανική Πληροφορική και τι τεχνικές εφαρμόζονται.

Πολλές ιδιωτικές εταιρείες αλλά και Δημόσιοι οργανισμοί ελέγχουν τους υπολογιστές των εργαζομένων τους, όπως ηλεκτρονικό ταχυδρομείο, αρχεία που βρίσκονται στον σκληρό δίσκο, ιστορικό περιηγήσεων στο Διαδίκτυο, έτσι ώστε να αποφευχθούν οι διαρροές ευαίσθητων προσωπικών δεδομένων ή εταιρικών πληροφοριών που μπορεί να έχουν αντίκτυπο στην ανταγωνιστικότητα μιας εταιρείας. Οι εισαγγελικές αρχές μπορούν να εκδώσουν εντάλματα έρευνας σε αρχεία και στο ηλεκτρονικό ταχυδρομείο ατόμων που θεωρούνται ύποπτα για ηλεκτρονική απάτη. Για να εξακριβωθεί ένα ηλεκτρονικό έγκλημα θα πρέπει αρχικά να γίνει η συλλογή όλων των απαραίτητων στοιχείων και στην συνέχεια η ανάλυση τους από τα δεδομένα του υπό εξέταση πληροφοριακού συστήματος. Γίνεται εύκολα κατανοητό ότι είναι απαραίτητη η ύπαρξη μιας γενικά αποδεκτής μεθοδολογίας που θα επιτρέπει να εξετάζονται με αποτελεσματικό τρόπο οι διάφορες υποθέσεις ηλεκτρονικού εγκλήματος. Επιπροσθέτως, η μεθοδολογία αυτή θα πρέπει να είναι εύκολα προσαρμόσιμη και επεκτάσιμη ανάλογα με τις απαιτήσεις μιας έρευνας.

Οι Δικανικές μέθοδοι έχουν «κληρονομήσει» τα χαρακτηριστικά τους από τις διαδικασίες της φυσικής Δικανικής έρευνας. Για να γίνει ευκολότερα κατανοητή η διαδικασία μιας Δικανικής έρευνας θα γίνει παράθεση μιας γενικής διαδικασίας από το πραγματικό κόσμο στην περίπτωση ενός εγκλήματος. Αναλύοντας ένα έγκλημα στο φυσικό κόσμο, όπως για παράδειγμα μια ληστεία, παρατηρούμε ότι η διαδικασία αποτελείται από πέντε βασικά βήματα. Αρχικά, μόνο άτομα που έχουν ειδική εκπαίδευση και γνώσεις έχουν πρόσβαση στο χώρο του εγκλήματος έτσι ώστε να εκκινήσουν την διαδικασία συλλογής και έλεγχου των πειστηρίων. Στη συνέχεια, ο χώρος του εγκλήματος απομονώνεται. Οι ειδικοί συλλέγουν τα απαραίτητα στοιχειά προσπαθώντας να κατανοήσουν το περιβάλλον του εγκλήματος. Η συλλογή των απαραίτητων πειστηρίων γίνεται βάση κάποιων ερωτημάτων που θα πρέπει να απαντηθούν από τους ειδικούς. Ερωτήματα που αφορούν το λόγο της επίθεσης, τον αριθμό των ατόμων που συμμετείχαν στην εγκληματική ενέργεια, αν υπάρχουν τυχόν ίχνη και αυτόπτες μάρτυρες είναι μερικά από αυτά που θα πρέπει να απαντηθούν έτσι ώστε να γίνει επαρκής συλλογή των απαραίτητων στοιχείων. Διάφορα τεχνολογικά μέσα όπως ψηφιακές φωτογραφίες ή και δαχτυλικά αποτυπώματα. Στην συνέχεια όλα τα απαραίτητα στοιχεία μεταφέρονται σε ειδικά εργαστήρια όπου γίνεται η ανάλυση τους. Στο τελικό στάδιο και μετά την μελέτη των στοιχείων που έχουν συλλεχθεί, εκδίδεται πόρισμα με το οποίο οι διάφορες αρμόδιες αρχές διενεργούν διώξεις, σύμφωνα με ό,τι ορίζει η νομοθεσία του κράτους για το συγκεκριμένο έγκλημα. Γίνεται εύκολα αντιληπτό ότι έχει δημιουργηθεί μια γενική μέθοδος που προσαρμόζεται αναλόγως με την υπάρχουσα εγκληματική ενέργεια αλλά και την νομοθεσία που ορίζεται από κάθε κράτος. Η επιστήμη της Δικανικής Πληροφορικής «προσπάθησε» να κληρονομήσει από τις διαδικασίες συλλογής στοιχείων των φυσικών μεθόδων έτσι ώστε να δημιουργηθεί ένα πανομοιότυπο – ευέλικτο πλαίσιο ψηφιακών μεθοδολογιών που θα προσαρμόζεται ανάλογα με το ηλεκτρονικό έγκλημα που βρίσκεται υπό διερεύνηση.

3.1 Γενικές πρακτικές μεθοδολογίας ανάλυσης «Δικανικής Πληροφορικής»

Οποιοδήποτε πληροφοριακό σύστημα μπορεί να αποτελέσει μέρος όπου μπορεί να διεξαχθεί παράνομη ηλεκτρονική εγκληματική ενέργεια. Συχνό καθημερινό φαινόμενο αποτελεί πληροφοριακά συστήματα εταιρειών να πέφτουν θύματα ηλεκτρονικών εγκλημάτων, έχοντας σαν αποτέλεσμα την απώλεια σημαντικών ευαίσθητων δεδομένων η οποία έχει οικονομικές

επιπτώσεις στην εταιρεία που έπεσε θύμα της ηλεκτρονικής απάτης. Όπως συμβαίνει στην διεξαγωγή έρευνας ενός πραγματικού-φυσικού εγκλήματος και όπως αυτό έχει περιγράφει στην προηγούμενη ενότητα, έτσι και στην διεξαγωγή έρευνας μιας ηλεκτρονικής εγκληματικής ενέργειας ακολουθούνται κάποια βασικά βήματα μιας γενικής μεθόδου.

Αξίζει να σημειωθεί ότι πολλές εταιρίες αλλά και δημόσιοι φορείς, χρησιμοποιούν στα πληροφοριακά τους συστήματα υπηρεσίες Web (Web Services).Οι υπηρεσίες αυτές χρησιμοποιούνται για την αυτοματοποίηση εσωτερικών διαδικασιών όπως για παράδειγμα ένα Web Service που φέρνει αποτελέσματα επί των πωλήσεων ενός αγαθού με την μορφή μιας αναφοράς (report), συνδυάζοντας ερωτήματα που γίνονται σε μια βάση δεδομένων ή και ακόμα υπηρεσίες που τρέχουν σε πραγματικό χρόνο ηλεκτρονικούς διαγωνισμούς φέρνοντας τα στοιχεία των επιτυχόντων. Όπως γίνεται εύκολα κατανοητό αυτές οι υπηρεσίες Ιστού πολλές φορές είναι προσβάσιμες από το Διαδίκτυο πέρα από το ad-hoc περιβάλλον μιας εταιρείας, κάτι που τις καθιστά ευάλωτες σε επιθέσεις με τον κίνδυνο να αποσπαστούν ευαίσθητες πληροφορίες από προσωπικά δεδομένα μέχρι οικονομικά στοιχεία. Η επιτακτική ανάγκη ύπαρξης των υπηρεσιών Ιστού στα σύγχρονα πληροφοριακά συστήματα καθιστά απαραίτητη, στην περίπτωση ηλεκτρονικού εγκλήματος, την ύπαρξη γενικής μεθοδολογίας που θα προλαμβάνει επιθέσεις τέτοιο τύπου.

Μια μέθοδος ανεύρεσης ψηφιακών πειστηρίων θα πρέπει να πληροί τις κάτωθι γενικές απαιτήσεις:

- Η μεθοδολογία θα πρέπει να είναι γενική, έτσι ώστε να παραμένει ανεπηρέαστη από τις διάφορες τεχνολογικές αλλαγές.
- Δεύτερη προϋπόθεση είναι ότι η μέθοδος θα πρέπει να είναι εύκολα υλοποιήσιμη-πρακτική, ακολουθώντας γενικές μεθόδους συλλογής των απαραίτητων στοιχείων όπως και σε μια φυσική διαδικασία.
- Η μεθοδολογία θα πρέπει να είναι εύκολα προσαρμόσιμη στα δεδομένα ανάλογα με την μορφή του εγκλήματος και το περιβάλλον που αυτό έχει διαπραχτεί.
- Τέλος, μια μεθοδολογία θα πρέπει να είναι δομημένη, δηλαδή να τυποποιείται εύκολα, συνολικά ή εν μέρει με την μορφή κάποιου εργαλείου.

Όπως προαναφέρθηκε κάθε πληροφοριακό σύστημα μπορεί να θεωρηθεί σαν χώρος ενός ηλεκτρονικού εγκλήματος. Αρχικά ο χώρος αυτός θα πρέπει να απομονωθεί από το περιβάλλον έτσι ώστε να μην υποστεί καμία αλλαγή. Πρώτο μέλημα του ειδικού επιστήμονα θα είναι να συλλέξει ένα αντίγραφο ασφαλείας του πληροφοριακού συστήματος που δέχθηκε την ηλεκτρονική επίθεση, έτσι ώστε στην περίπτωση καταστροφής ή απώλειας των δεδομένων να μπορεί να γίνει επαναφορά του συστήματος σε προηγούμενη πλήρως λειτουργική κατάσταση. Στην συνέχεια ο ειδικός ερευνητής σε συνεργασία με τον υπεύθυνο του πληροφοριακού συστήματος της εταιρείας και αφού έχει πάρει τα απαραίτητα αντίγραφα ασφαλείας, θα κληθεί να συλλέξει βάση κάποιας μεθοδολογίας και με την βοήθεια ειδικών εργαλείων τα απαραίτητα ψηφιακά πειστήρια. Όλοι οι επαγγελματίες που εμπλέκονται σε μια εγκληματολογική εξέταση έχουν μια τις παρακάτω εγκληματολογικές και ηθικές ευθύνες (7):

- Να διατηρεί την αντικειμενικότητα του.
- Να παρουσιάζει τα γεγονότα με ακρίβεια.
- Να μην κάνει παρακράτηση στοιχείων, κάτι που θα οδηγήσει στην αλλοίωση των αποτελεσμάτων.

- Θα πρέπει να προβάλουν στοιχεία τα οποία θα έχουν κάποια βάση και θα αποδεικνύονται.

Επιπροσθέτως, κατά την διάρκεια μιας εγκληματολογικής εξέτασης ο ειδικός ερευνητής της Δικανικής Πληροφορικής θα πρέπει να κάνει τις εξής ενέργειες:

- Θα πρέπει να εφαρμόζουν όλες τις διαδικαστικές αρχές για την συλλογή ψηφιακών ενδείξεων.
- Να μην εκτελέσει οποιαδήποτε ενέργεια που θα μπορούσε να αλλοιώσει τα αποδεικτικά στοιχεία.
- Μόνο ειδικευμένα πρόσωπα θα πρέπει να έχουν πρόσβαση στις ψηφιακές ενδείξεις.
- Ο ειδικός επιστήμονας θα πρέπει να καταγράφει όλες τις δραστηριότητες που σχετίζονται με την πρόσβαση, την αποθήκευση, την μεταφορά των ψηφιακών δεδομένων και να διαφυλάσσει σε ένα αρχείο (record). Στην συνέχεια όλες οι τεκμηριωμένες διαδικασίες θα πρέπει να επαναληφθούν ώστε να επιτευχτεί το ίδιο αποτέλεσμα.
- Ο ειδικός της εγκληματολογικής εξέτασης είναι υπεύθυνος για όλες τις δράσεις που σχετίζονται με την συλλογή των ψηφιακών πειστηρίων. Ως υπεύθυνος θα πρέπει να εξασφαλίζει να γίνεται χρήση όλων των βέλτιστων πρακτικών που θα επιφέρουν τα επιθυμητά αποτελέσματα.

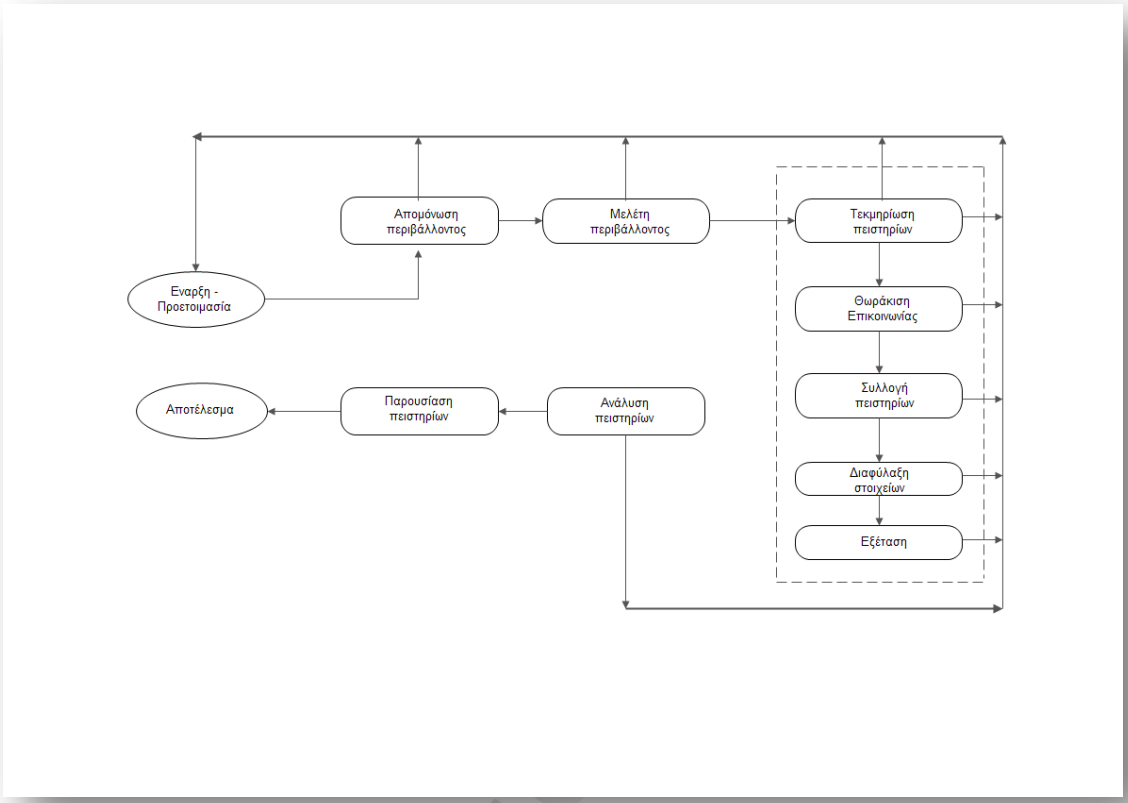
Επίσης σε μια Δικανική έρευνα θα πρέπει να τηρούνται οι εξής τέσσερις βασικές αρχές από τους ειδικούς ερευνητές (7)*:*

- Θα πρέπει να διατηρούνται τα δεδομένα ακέραια καθώς και τα δεδομένα γνησιότητας.
- Θα πρέπει να γίνεται πρόληψη για τυχόν κίνδυνο μόλυνσης των δεδομένων.
- Τα όποια αποτελέσματα θα πρέπει να παρουσιάζονται εγγράφως σωστά δομημένα και με την απαραίτητη τεκμηρίωση.
- Τέλος, θα πρέπει να γίνεται χρήση μιας συστηματικής , επιστημονικής μεθοδολογίας.

Μετά την συλλογή των πειστηρίων, αυτά μεταφέρονται με την χρήση διάφορων ψηφιακών μέσων, όπως σκληροί δίσκοι, usb flash δίσκων σε μορφή images, σε ειδικά εργαστήρια έτσι ώστε να αναλυθούν περεταίρω με την χρήση διάφορων τεχνολογικών μέσων. Εφόσον θεωρηθεί απαραίτητο οι εδικοί ερευνητές κατασκευάζουν πανομοιότυπο περιβάλλον με αυτό του πληροφοριακού συστήματος έτσι ώστε να γίνει προσομοίωση της ηλεκτρονικής επίθεσης και να ερευνηθεί η προέλευση της καθώς και οι υπαίτιοι αυτής.

Στο τελικό στάδιο της Δικανικής έρευνας και αφού έχουν ολοκληρωθεί όλα τα βήματα που ορίζει η μεθοδολογία που έχει επιλεχθεί, τα στοιχεία που έχουν αναλυθεί δίνονται στις εισαγγελικές αρχές υπό την μορφή του πορίσματος, συμπεριλαμβάνοντας τα αποδεικτικά στοιχεία και τα συμπεράσματα για την διάπραξη του εγκλήματος και τους πιθανούς δράστες. Τα δεδομένα που παρέχονται στις εισαγγελικές αρχές δεν θα πρέπει να έχουν αλλοιωθεί κατά την ανάλυση τους διότι σε διαφορετική περίπτωση τίθεται θέμα αμφισβήτησης τους από τις δικαστικές αρχές. Τέλος εφαρμόζεται η νομοθεσία που ορίζεται από το κάθε κράτος.

Στο σχήμα που ακολουθεί αποτυπώνονται διαγραμματικά τα βήματα μιας γενικής μεθόδου της Δικανικής Πληροφορικής κατά την διεξαγωγή μιας εγκληματικής έρευνας (8).



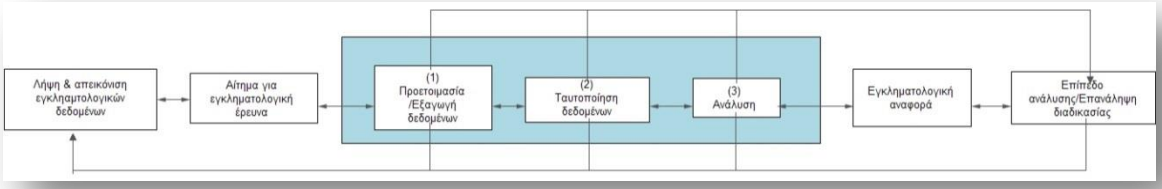
Εικόνα 5. Στάδια έρευνας Δικανικής Υπολογιστικής.

3.1.1 Μεθοδολογία τριών βημάτων

Στην εν λόγω ενότητα θα γίνει περιγραφή μιας μεθοδολογίας Δικανικής Υπολογιστικής που περιλαμβάνει τρία κυρίως βήματα όπως αυτή έχει δημοσιευτεί από το Υπουργείο Αμύνης των Ηνωμένων Πολιτειών τον Ιανουάριο του 2008 (9). Σύμφωνα με την συγκεκριμένη μεθοδολογία υπάρχουν τα εξής στοιχεία «κλειδιά» στην Δικανική Πληροφορική που θα πρέπει να λαμβάνονται υπ' όψιν:

- Η χρήση επιστημονικών μεθόδων.
- Η συλλογή και φύλαξη των διαφόρων δεδομένων της έρευνας.
- Η επικύρωση των στοιχείων που έχουν ερευνηθεί.
- Η εξακρίβωση τους.
- Η ανάλυση και ερμηνεία τους.
- Τέλος, η έγγραφη τεκμηρίωση τους και η παρουσίαση τους στις εισαγγελικές αρχές.

Η μέθοδος, όπως προαναφέρθηκε, αποτελείται από τρία κυρίως βήματα όπως φαίνεται και στο σχήμα που ακολουθεί.



Εικόνα 6. Σχεδιάγραμμα μεθοδολογίας τριών βημάτων (9).

Όπως παρατηρείται τα κυρίως βήματα που συμπεριλαμβάνονται στο μπλε πλαίσιο της διαδικασίας είναι τα εξής:

- Προετοιμασία του πληροφοριακού συστήματος (χώρου όπου έγινε η ηλεκτρονική απάτη) και εξαγωγή των δεδομένων από αυτό.
- Ταυτοποίηση των γνήσιων δεδομένων.
- Ανάλυση των ψηφιακών πειστηρίων.

Στις επόμενες παραγράφους θα δοθεί λεπτομερέστερη περιγραφή των βημάτων αυτών.

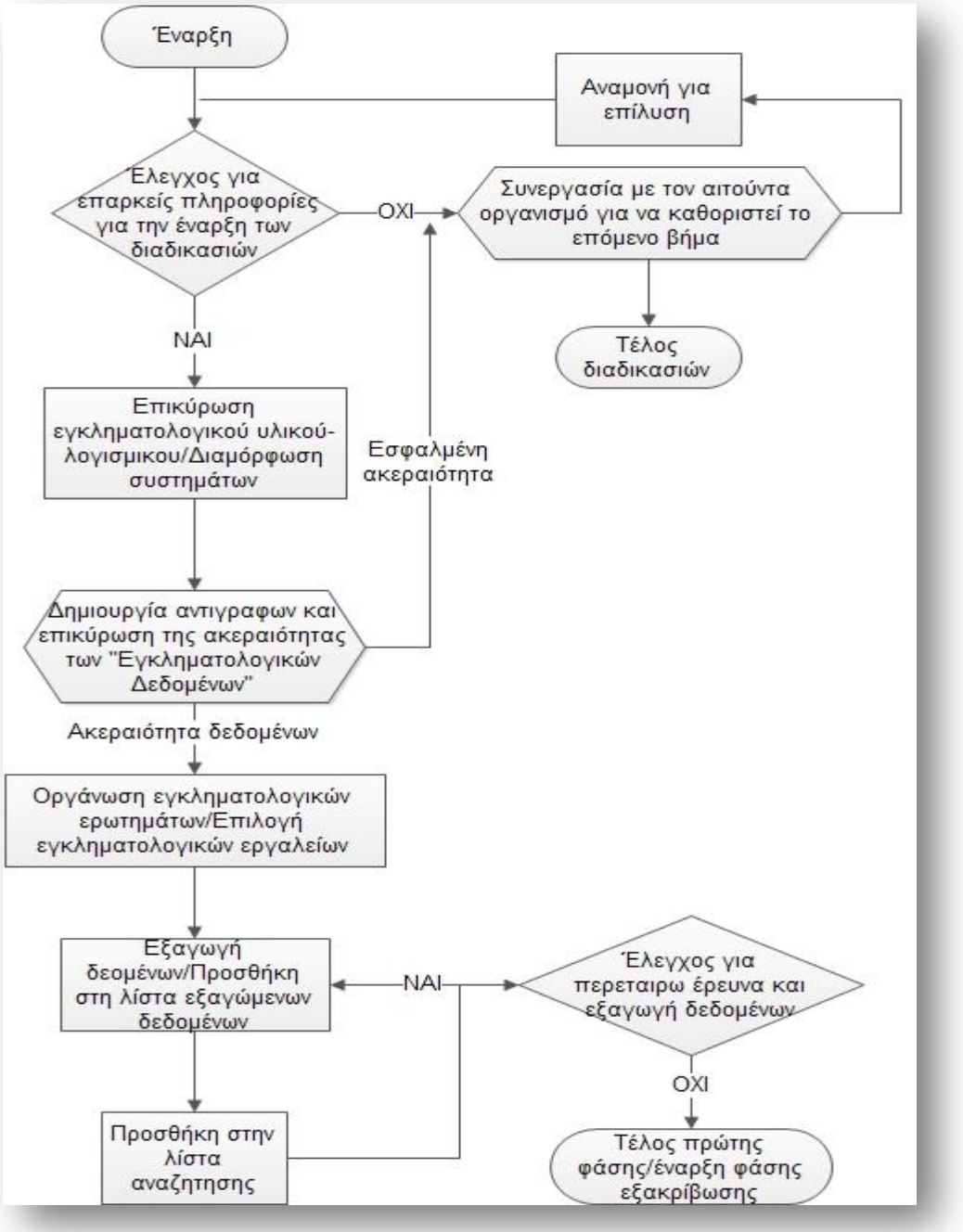
Προετοιμασία-Εξαγωγή αποδεικτικών στοιχείων

Το πρώτο βήμα σε κάθε δικανική έρευνα είναι η επικύρωση της καλής λειτουργίας όλων των υπολογιστικών μηχανημάτων (hardware) και όλων των λογισμικών(software) του πληροφοριακού περιβάλλοντος. Θεωρείται απαραίτητο για ένα οργανισμό να επικυρώνει την καλή λειτουργία όλων των μηχανημάτων και των λογισμικών της μετά από την αγορά τους και πριν την κανονική λειτουργία τους. Επιπροσθέτως θα πρέπει να γίνεται έλεγχος καλής λειτουργίας μετά από κάθε ενημέρωση του λογισμικού (update, patching) ή αναδιαμόρφωση του πληροφοριακού περιβάλλοντος.

Αρχικά, ο ειδικός ερευνητής δημιουργεί αντίγραφα των εγκληματολογικών δεδομένων και επικυρώνει ότι δεν έχουν υποστεί κάποια αλλοίωση. Η προηγούμενη διαδικασία ακολουθεί όλες τις νόμιμες διαδικασίες, όπως ορίζονται από την σχετική νομοθεσία , για να δημιουργηθεί ένα ακριβές αντίγραφο των εγκληματολογικών δεδομένων. Το εικονικό αρχείο αποτελεί bit προς bit ακριβές αντίγραφο των γνήσιων δεδομένων, χωρίς καμία προσθήκη ή να έχει υποστεί γενικότερα κάποια αλλαγή. Επίσης το αντίγραφό θα πρέπει να είναι πλήρως λειτουργικό διότι τα ψηφιακά πειστήρια που θα εξαχθούν θα παρουσιαστούν σε μια δικαστική αίθουσα. Για επιβεβαιώσουν οι ερευνητές ότι τα δεδομένα δεν έχουν αλλοιωθεί χρησιμοποιούν τεχνικές όπως να επαληθεύσουν τα δεδομένα με την χρήση hash συναρτήσεων ή ψηφιακό αποτύπωμα των στοιχείων.

Μετά την επαλήθευση της ακεραιότητας των δεδομένων που πρέπει να αναλυθούν, θα πρέπει να γίνουν οι σωστές διαδικασίες για την εξαγωγή των δεδομένων. Στη συνέχεια τα αιτήματα της εγκληματολογικής έρευνας οργανώνονται σε ερωτήματα που θα λάβουν στην συνέχεια απαντήσεις για την μορφή της ψηφιακής επίθεσης. Οι ειδικοί ερευνητές επιλέγουν τα κατάλληλα εργαλεία για την διεξαγωγή της εγκληματολογικής έρευνας. Συνήθης πρακτική των εξεταστών είναι να συντάσσουν «Λίστα αναζήτησης-αποτελεσμάτων» η οποία είναι μια τρέχουσα λίστα των αντικειμένων που ζητούνται κατά την έρευνα, για παράδειγμα «έλεγχος για είσοδο στο πληροφοριακό σύστημα από μη εξουσιοδοτημένο χρήστη». Καθώς προχωράει η έρευνα οι διάφορες διαδικασίες της λίστας μαρκάρονται σαν «υπό επεξεργασία» ή ως «ολοκληρωμένες».

Όποια δεδομένα και αποτελέσματα εξάγονται κατά την έρευνα, σύμφωνα με αυτά που ζητούνται στην πρώτη λίστα, προσθέτονται σε μια δεύτερη λίστα η οποία ονομάζεται «Λίστα εξαγόμενων δεδομένων». Στη επόμενη φάση της μεθοδολογίας γίνεται η εξακρίβωση των δεδομένων, που θα περιγραφεί στην επόμενη παράγραφο. Το λογικό διάγραμμα των διαδικασιών της προετοιμασίας και της εξαγωγής των αποδεικτικών δεδομένων δίνεται στην (Εικόνα 7).



Εικόνα 7. Φάση προετοιμασίας-εξαγωγής αποδεικτικών στοιχείων

Εξακρίβωση Δεδομένων

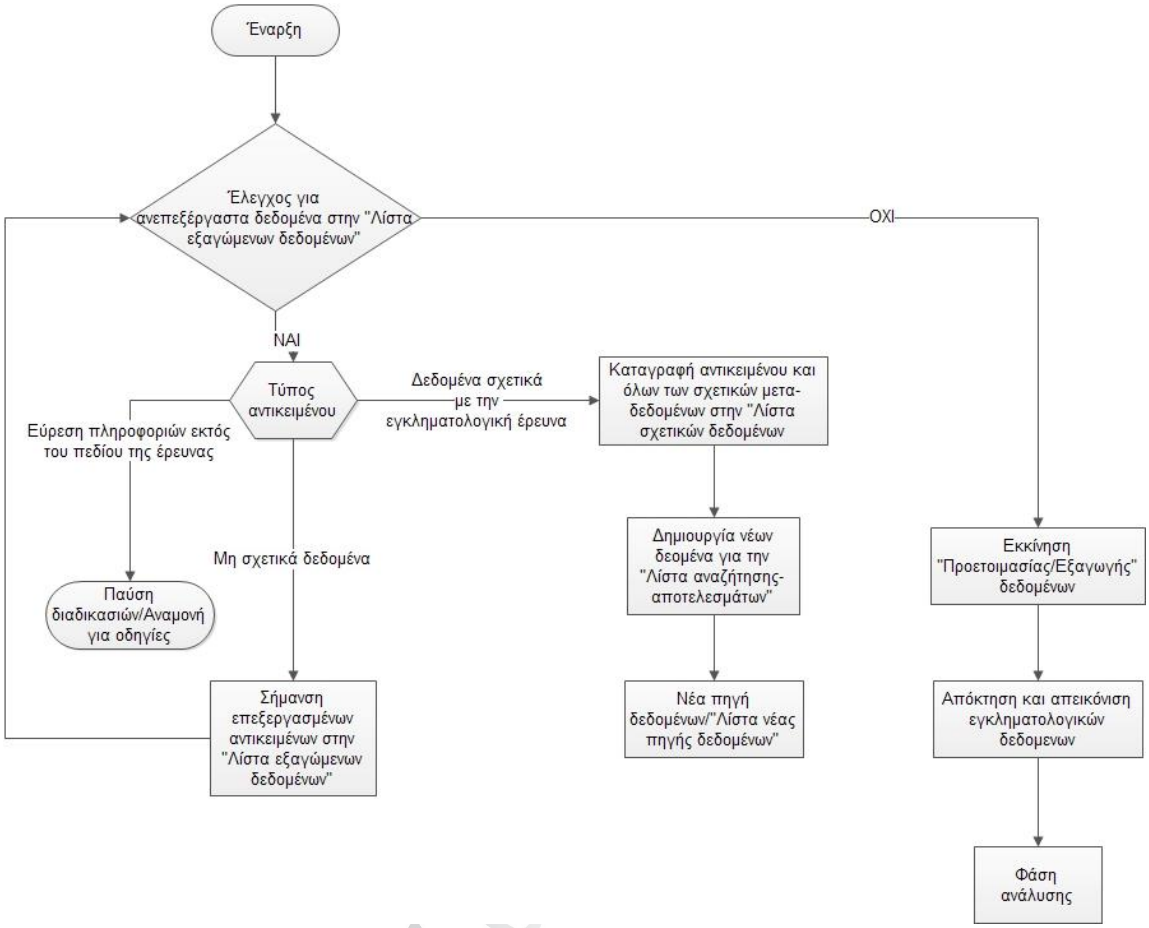
Οι ερευνητές της εγκληματολογικής έρευνας επαναλαμβάνουν την διαδικασία της εξακρίβωσης για κάθε αντικείμενο της «Λίστας εξαγόμενων δεδομένων». Αρχικά, προσδιορίζεται τι τύπος αντικειμένου ερευνάτε, αν το αντικείμενο δεν έχει σχέση με την εγκληματολογική έρευνα «μαρκάρετε» σαν επεξεργασμένο και η διαδικασία συνεχίζεται. Σε κάθε περίπτωση όταν ο εγκληματολογικός ερευνητής εντοπίσει ένα ενοχοποιητικό στοιχείο το οποίο είναι έξω από το πεδίο της έρευνας κάθε δραστηριότητα σταματάει και μετά από συνεννόηση με τον αιτούμενο αποφασίζονται ποια βήματα θα ακολουθηθούν περαιτέρω. Για να γίνει πιο κατανοητό σε μια υποτιθέμενη έρευνα για οικονομικό έγκλημα εντοπιστούν στοιχεία διακίνησης- πειρατείας παράνομου λογισμικού, η έρευνα παίρνει έκταση εκτός του αρχικού πεδίου. Συνήθης τακτική είναι η αρχική έρευνα να σταματάει και να η επιδιώκεται νομικά η διεύρυνση της έρευνας ή να ληφθεί ένα δεύτερο ένταλμα για ξεχωριστή εγκληματική διερεύνηση.

Αν ένα αντικείμενο είναι σχετικό με την έρευνα προστίθεται σε μια τρίτη λίστα η οποία ονομάζεται «Λίστα σχετικών δεδομένων». Στην εν λόγω λίστα μπορεί να εμπεριέχονται δεδομένα όπως η ταυτότητα των δραστών, εικόνες, δεδομένα σχετικά με αριθμούς κοινωνικής ασφάλισης ή e-mails σχετικά που δίνουν στοιχεία για την επίθεση. Υπάρχει πάντα η πιθανότητα πολλά αντικείμενα να δημιουργούν νέα δεδομένα προς έρευνα. Σε μια τέτοια περίπτωση ο ειδικός ερευνητής θα πρέπει να προσθέσει τα νέα αντικείμενα στην «Λίστα αναζήτησης-αποτελεσμάτων» εκ νέου έτσι ώστε τα νέα δεδομένα να αναλυθούν.

Σε μια εγκληματολογική εξέταση μπορεί να καταδείξει πολλούς διαφορετικούς τύπους νέων αποδεικτικών στοιχείων. Τα αρχεία πρόσβασης (access logs), firewall logs, αποτελούν περαιτέρω δεδομένα για έναν εγκληματολογικό ερευνητή, τα οποία προστίθενται σε μια τέταρτη κατά σειρά λίστα «Νέα Πηγή της λίστας δεδομένων».

Μετά την επεξεργασία των δεδομένων που προέρχονται από την «Λίστα εξαγόμενων δεδομένων», οι εξεταστές πηγαίνουν στο προηγούμενο βήμα και ελέγχουν τυχόν νέα δεδομένα που έχουν προκύψει στην «Λίστα αναζήτησης-αποτελεσμάτων». Ομοίως, για κάθε νέα πηγή δεδομένων, που πιθανόν οδηγούν σε νέα αποδεικτικά στοιχεία, ο εξεταστής επαναλαμβάνει όλη την διαδικασία από την αρχή, απόκτησης και απεικόνισης (imaging) των νέων εγκληματολογικών δεδομένων.

Ανάλογα με το στάδιο της υπόθεσης, τα εξαγόμενα δεδομένα που σχετίζονται με την υπόθεση μπορεί να δίνουν αρκετές πληροφορίες για να τερματίσει η διαδικασία της έρευνας. Για παράδειγμα αν τα στοιχεία αποκαλύψουν την ταυτότητα του δράστη της ψηφιακής επίθεσης και επιτρέπουν να οδηγηθεί ο υπαίτιος στις Δικαστικές αίθουσες δεν απαιτείται περαιτέρω εγκληματολογική ανάλυση των πειστηρίων. Στην περίπτωση που τα εξαγόμενα που έχουν συλλεχθεί δεν είναι αρκετά, τότε ο ειδικός ερευνητής προχωράει στο επόμενο βήμα της μεθοδολογίας που είναι αυτό της ανάλυσης των δεδομένων. Το λογικό διάγραμμα της Εικόνα 8. Φάση Εξακρίβωσης Δεδομένων που ακολουθεί περιγράφει τις ανωτέρω διαδικασίες.



Εικόνα 8. Φάση Εξακρίβωσης Δεδομένων

Ανάλυση Δεδομένων

Η φάση της ανάλυσης των δεδομένων που έχουν συλλεχθεί, αποτελεί το τελευταίο μέρος της εγκληματολογικής μεθόδου. Για κάθε αντικείμενο της λίστας των σχετικών με την έρευνα δεδομένων, οι ερευνητές καλούνται να απαντήσουν σε ερωτήματα όπως ποιος, τι , πότε, που και πως έγινε η ψηφιακή επίθεση. Επιπροσθέτως, οι εξεταστές προσπαθούν να εξηγήσουν ποιος χρήστης ή εφαρμογή δημιούργησε, επεξεργάστηκε, δέχτηκε ή έστειλε το κάθε αντικείμενο και πως αρχικά εμφανίστηκαν. Τέλος, θα πρέπει να εξηγηθεί πως οι πληροφορίες αυτές είναι σημαντικές για την επίλυση της υπόθεσης.

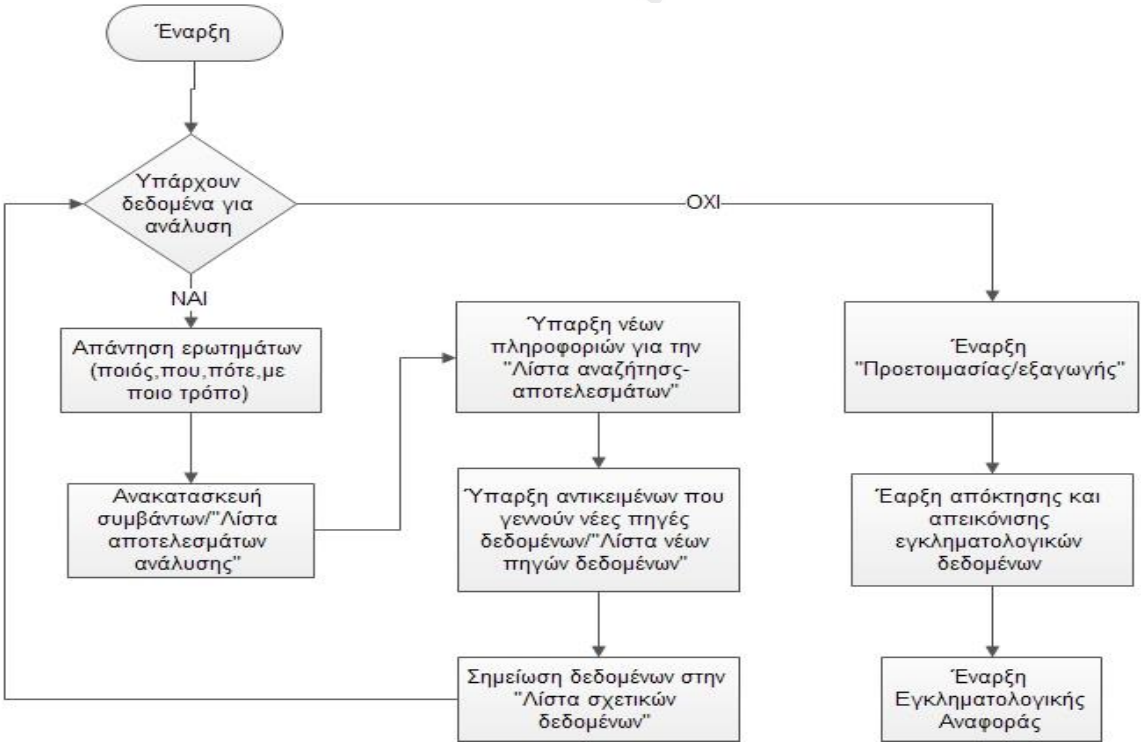
Σκοπός της μεθόδου της ανάλυσης είναι να ανακατασκευαστεί το συμβάν της επίθεσης παράγοντας ένα χρονοδιάγραμμα που περιγράφει το ιστορικό της επίθεσης. Για κάθε σχετικό στοιχείο, οι εξεταστές προσπαθούν να εξηγήσουν πότε δημιουργήθηκε, πότε προσπελάστηκε, τροποποιήθηκε, διαγράφηκε, λήφθηκε ή διαβάστηκε. Παρατηρείται και εξηγείται η ακολουθία των συμβάντων που έλαβαν χώρα, σημειώνοντας τα γεγονότα που συνέβησαν την ίδια χρονική στιγμή.

Στο επόμενο βήμα, οι ερευνητές καταγράφουν όλη την ανάλυση των δεδομένων και των πληροφοριών που σχετίζονται με την εγκληματολογική έρευνα, προσθέτοντας τα σε μια πέμπτη

λίστα την «Λίστα ανάλυσης αποτελεσμάτων». Οι πληροφορίες που υπάρχουν στην εν λόγω λίστα ικανοποιούν όλα τα ερωτήματα που «γεννάει» η έρευνα όπως ποιος, που, πότε και με ποιόν τρόπο έγινε η εγκληματική ενέργεια. Ακόμα και στο τελευταίο στάδιο της ανάλυσης μπορεί να δημιουργηθούν νέες πηγές δεδομένων προς έλεγχο. Σε μια τέτοια περίπτωση ακολουθούνται οι προηγούμενες διαδικασίες ελέγχου και εξαγωγής των δεδομένων όπως περιγράφηκαν στις προηγούμενες ενότητες, έτσι ώστε τα νέα στοιχεία να εξεταστούν ενδελεχώς.

Στο τελικό στάδιο της μεθοδολογίας και εφόσον τα βήματα έχουν επαναληφθεί αρκετές φορές έτσι ώστε τα αποτελέσματα να ανταποκρίνονται στις απαιτήσεις της εγκληματολογικής έρευνας, ακολουθεί η φάση της «Εγκληματολογικής αναφοράς». Σε αυτό το στάδιο οι εξεταστές δίνουν σε έγγραφη μορφή τα πειστήρια έτσι ώστε να γίνονται κατανοητά στους αιτούντες του οργανισμού που δέχθηκε την επίθεση και να μπορέσουν να τα χρησιμοποιήσουν στην υπόθεση. Η τελική αναφορά είναι ο καλύτερος τρόπος για τους εξεταστές για να κοινοποιήσουν τα πορίσματα τους για τους αιτούντες. Μετά την αναφορά, ο αιτών κάνει περιπτωσιολογική ανάλυση που ερμηνεύει τα ευρήματα σύμφωνα με το πλαίσιο της υπόθεσης. Στην εικόνα δίνεται το διάγραμμα των διαδικασιών της φάσης της ανάλυσης.

Αξίζει να επισημανθεί ότι κατά την διάρκεια της εξέτασης, τα βήματα μπορεί να επαναληφθούν πολλές φορές. Όταν τα συγκεντρωθέντα αποδεικτικά στοιχεία είναι επαρκή για ποινική δίωξη, η ανάγκη για περαιτέρω ταυτοποίηση και ανάλυση των στοιχείων μειώνεται με αποτέλεσμα η εγκληματολογική εξέταση να λαμβάνει τέλος.



Εικόνα 9. Φάση Ανάλυσης Δεδομένων

3.1.2 Μεθοδολογία Πολλαπλών Συνιστωσών (Gobler-Louwrens-Solms)

Πολλοί οργανισμοί ξοδεύουν μεγάλα χρηματικά ποσά και χρόνο έτσι ώστε να ασφαλίσουν τα πληροφοριακά τους συστήματα από παραβιάσεις ασφαλείας ή φυσικές καταστροφές με την χρήση σχεδίων αποκατάστασης των πληροφοριακών συστημάτων από τέτοιου είδους επικείμενες καταστροφές καθώς επίσης και από σχέδια συνεχούς λειτουργίας της εταιρείας. Τα εν λόγω σχέδια βοηθούν έναν οργανισμό να αναγνωρίσει ένα τέτοιο γεγονός καταστροφής ή επίθεσης στο πληροφοριακό σύστημα έτσι ώστε να το αντιμετωπίσει έγκαιρα, βρίσκοντας την βέλτιστη λύση για την γρηγορότερη ανάκαμψη λειτουργιών της εταιρείας. Σε μια ενδεχόμενη επίθεση τα συστήματα ανίχνευσης εισβολέων (IDS-Intrusion Detection Systems), καταγράφουν μερικές πληροφορίες που πολλές φορές δεν περιέχουν αρκετά και αξιόπιστα και αποδεκτά στοιχεία για να παρουσιαστούν στην Δικαστική αίθουσα. Ελάχιστοι οργανισμοί έως σήμερα επένδυαν χρηματικά ποσά για να προσαρμόσουν συστήματα διαχείρισης και υποδομής που θα βοηθήσουν σε μια ενδεχόμενη ψηφιακή έρευνα. Με την εξέλιξη της τεχνολογίας η φύση των επιθέσεων στα διάφορα πληροφοριακά συστήματα έχει αλλάξει. Οι σημερινές εγκληματολογικές έρευνες απαιτούν αποδεκτά «ζωντανά» ψηφιακά πειστήρια, όπως για παράδειγμα αρχεία swap, δικτυακές λειτουργίες, web εφαρμογές, έτσι ώστε να προσδιορίσει την ρίζα του συμβάντος και να ασκηθεί δίωξη κατά των δραστών.

Το 2010 προτάθηκε μια διαφορετική μεθοδολογία από ερευνητές του Πανεπιστημίου του Γιοχάνεσμπουργκ στην Ψηφιακή εγκληματολογία (Digital Forensics) (10). Η νέα προσέγγιση περιλαμβάνει τρείς κυρίως φάσεις καθώς και μερικές επιμέρους φάσεις. Ιδιαίτερη βαρύτητα δίνεται στην συλλογή πειστηρίων “live” επιθέσεων, σε αντίθεση με τις παραδοσιακές μεθόδους της Δικανικής Υπολογιστικής. Η μέθοδος αποτελείται από τρείς συνιστώσες:

- Την προληπτική ψηφιακή εγκληματολογία (Proactive Digital Forensics), που αφορά όλες τις διαδικασίες που θα πρέπει να ληφθούν υπόψη για την προληπτική χρήση της ψηφιακής εγκληματολογίας σε ένα πληροφοριακό σύστημα, έτσι ώστε να υπάρχουν πάντα αποδεικτικά στοιχεία σε μια επικείμενη επίθεση.
- Την ενεργή ψηφιακή εγκληματολογία (Active Digital Forensics), η οποία αφορά την «ζωντανή» εγκληματολογία(“live” forensics).
- Την δραστική ψηφιακή εγκληματολογία(Reactive Digital Forensics), που αφορά την μη «ενεργή» εγκληματολογία (“dead” forensics).

3.1.2.1 Προληπτική Ψηφιακή Εγκληματολογία (Proactive Digital Forensics)

Η προληπτική ψηφιακή εγκληματολογία (Proactive Digital Forensics), καθορίζει τις διαδικασίες και τις τεχνολογίες, για την δημιουργία, τη συλλογή, τη διατήρηση και τη διαχείριση των ψηφιακών πειστηρίων, με στόχο να διευκολύνει μια επιτυχή και αποτελεσματική έρευνα με ελάχιστο κόστος. Επιπροσθέτως, προνοείται η μη διακοπή των επιχειρησιακών δραστηριοτήτων και εργασιών επιδεικνύοντας παράλληλα καλή εταιρική διακυβέρνηση.

Αρχικά το πληροφοριακό σύστημα θα πρέπει να βρίσκεται σε κατάσταση ετοιμότητας σε μια ενδεχόμενη έρευνα, αναλυτικότερα θα πρέπει να καλύπτει τις εξής απαιτήσεις:

1. Να παρέχει και να έχει προετοιμάσει όλη την υποδομή του πληροφοριακού συστήματος (συστήματα, δίκτυα), έτσι ώστε να υποστηρίζουν και να διευκολύνουν έρευνες της ψηφιακής μεθοδολογίας.

2. Δεύτερο στόχο αποτελεί η ανάπτυξη ενός σχεδίου διαχείρισης που θα εστιάζει στην αναγνώριση, συλλογή, διαχείριση, ανάκτηση και αρχειοθέτηση των ψηφιακών πειστηρίων. Τα ψηφιακά πειστήρια θα πρέπει να περιέχουν όλες αυτές τις πληροφορίες που θα διαμορφώνουν τον ψηφιακό χάρτη των αποδείξεων, όπως για παράδειγμα: κατηγορία του εγκλήματος, τόπος και χρόνος διεξαγωγής της εγκληματικής ενέργειας, πολιτικές διαχείρισης των αποδεικτικών στοιχείων.
3. Τρίτη προϋπόθεση είναι η ανάπτυξη οργανωτικών σχεδίων αντιμετώπισης κινδύνων. Για παράδειγμα η «τοποθέτηση» ενός εργαλείου IDS (Intrusion Detection System)[7].Με την εφαρμογή ενός εργαλείου IDS σε ένα πληροφοριακό σύστημα επιτυγχάνουμε την ενεργό παρακολούθηση των συστημάτων, δίνοντας την ευκαιρία να περιοριστούν οι κίνδυνοι από επιθέσεις σε «ζωντανά» συστήματα και να συλλεχτούν χρήσιμες πληροφορίες από μια ενδεχόμενη επίθεση, οι οποίες θα μπορέσουν να βοηθήσουν σε μια Δικανική έρευνα. Ένα σύστημα IDS επιτρέπει σε ένα οργανισμό να συμπεριληφθούν όλες οι απαιτήσεις για την συλλογή αποδεικτών στοιχείων σε μια διαδικασία εκτίμησης κινδύνου, να γίνει ανάλυση των επιχειρησιακών επιπτώσεων, διευκολύνει την ύπαρξη διαδικασιών επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών.
4. Τέταρτη απαίτηση είναι η ανάπτυξη ενός πλάνου που θα περιλαμβάνει την εκπαίδευση των εργαζομένων του οργανισμού πάνω στις διαδικασίες και τις έννοιες-ορισμούς της Δικανικής Πληροφορικής.
5. Απαραίτητη κρίνεται η ύπαρξη ενός πλάνου διαχείρισης που θα καθορίζει τον ρόλο και τις αρμοδιότητες που θα έχουν τόσο οι εσωτερικοί αλλά και οι εξωτερικοί εγκληματολογικοί ερευνητές.
6. Θα πρέπει να επικυρώνονται εγγράφως τα πρωτόκολλα έρευνας που θα ακολουθούνται σε μια έρευνα σύμφωνα με την βέλτιστη πρακτική μέθοδο.
7. Θα πρέπει να γίνεται κοστολόγηση της έρευνας.
8. Θα πρέπει να ελαχιστοποιηθούν οι όποιες διακοπές των επιχειρησιακών διαδικασιών κατά την διάρκεια της έρευνας.

Επόμενος στόχος της προληπτικής ψηφιακής εγκληματολογίας (Proactive Digital Forensics) είναι η ενίσχυση των προγραμμάτων διακυβέρνησης του οργανισμού. Θα πρέπει να παρέχονται αποτελεσματικοί έλεγχοι και μέτρα στα πληροφοριακά συστήματα της εταιρείας με στόχο την ασφάλεια των πληροφοριών του οργανισμού. Ένας οργανισμός έχει την δυνατότητα θα πρέπει να κάνει χρήση εργαλείων της ψηφιακής εγκληματολογίας(Digital Forensics),έτσι ώστε να αξιολογούνται οι έλεγχοι που εφαρμόζονται. Με την χρήση των εν λόγω εργαλείων θα απλοποιείται η διαδικασία μιας επικείμενης ψηφιακής έρευνας καθώς θα παρέχονται εξαρχής από τα ενσωματωμένα εργαλεία της ψηφιακής εγκληματολογίας στο πληροφοριακό σύστημα του οργανισμού τεκμηριωμένες αποδείξεις. Ο οργανισμός θα πρέπει να θέσει ένα άτομο το οποίο θα είναι υπεύθυνο και θα έχει την εξουσιοδότηση να χειρίζεται και να επιβλέπει τα εργαλεία αυτά και τις πληροφορίες που καταγράφονται. Τέλος θα πρέπει να οριστούν οι σχέσεις μεταξύ της ομάδας Ψηφιακής Εγκληματολογίας, Ασφάλειας Πληροφοριών, Ανάλυσης κινδύνου, Εσωτερικού Ελέγχου και των Νομικών υπηρεσιών του οργανισμού.

Τέλος, η προληπτική ψηφιακή εγκληματολογία (Proactive Digital Forensics) αποσκοπεί στην βελτίωση της αποτελεσματικότητας και της αποδοτικότητας των πληροφοριακών συστημάτων σε ένα οργανισμό με την χρήση εργαλείων της Ψηφιακής Εγκληματολογίας. Σύμφωνα με έρευνες το 2008 (11) το 41% των οργανισμών χρησιμοποιεί εργαλεία και τεχνικές της Ψηφιακής εγκληματολογίας(Digital Forensics) ως μέρος των μέτρων ασφαλείας των πληροφοριακών

[7] Ορισμός IDS: http://en.wikipedia.org/wiki/Intrusion_detection_system

συστημάτων. Στον πίνακα (10) που ακολουθεί παρουσιάζονται σε ποσοστιαίες μονάδες οι τεχνολογίες που χρησιμοποιούνται για την ασφάλεια των πληροφοριακών συστημάτων από διάφορους οργανισμούς κατά το έτος 2008.

Anti-virus software	97 %
Anti-spyware software	80 %
Application-level firewalls	53 %
Biometrics	23 %
Data loss prevention / content monitoring	38 %
Encryption of data in transit	71 %
Encryption of data at rest (in storage)	53 %
Endpoint security client software / NAC	34 %
Firewalls	94 %
Forensics tools	41 %
Intrusion detection systems	69 %
Intrusion prevention systems	54 %
Log management software	51 %
Public Key Infrastructure systems	36 %
Server-based access control lists	50 %
Smart cards and other one-time tokens	36 %
Specialized wireless security systems	27 %
Static account / login passwords	46 %
Virtualization-specific tools	29 %
Virtual Private Network (VPN)	85 %
Vulnerability / patch management tools	65 %
Web / URL filtering	61 %
Other	3 %

Εικόνα 10.Τεχνολογίες ασφαλείας. Πηγή CSI Computer Crime & Security Survey

Θεωρείται απαραίτητο να σχεδιάζονται εφαρμόζονται συστήματα και διαδικασίες με τέτοιο τόπο έτσι ώστε να διευκολύνουν μια Δικανική έρευνα. Για παράδειγμα η δομή των αρχείων(file structure) θα πρέπει να διευκολύνει την ανάκτηση των δεδομένων.

Ωστόσο, θα πρέπει να αποφεύγεται η μη εξουσιοδοτημένη χρήση των εργαλείων της Δικανικής Πληροφορικής όπως password crackers, εργαλεία anti-forensics ή data-hiding εργαλεία. Συνεπώς, κατά το στάδιο της προληπτικής ψηφιακής εγκληματολογίας (Proactive Digital Forensics) θα πρέπει ένας οργανισμός να προετοιμάσει το περιβάλλον για μια επικείμενη ψηφιακή έρευνα, να συμπεριλάβει όλες τις τεχνικές που θα ενισχύσουν και θα βελτιώσουν την λειτουργία του οργανισμού.

3.1.2.2 Δραστική Ψηφιακή Εγκληματολογία(Reactive Digital Forensics)

Η δραστική ψηφιακή εγκληματολογία(Reactive Digital Forensics), αφορά την έρευνα που λαμβάνει χώρα μετά από ένα περιστατικό επίθεσης. Όπως έχει προαναφερθεί τα πειστήρια αφορούν τη μη «ενεργή» εγκληματολογία (“dead” forensics). Η δραστική ψηφιακή εγκληματολογία περιλαμβάνει τέσσερις στόχους:

- Προσδιορίζει τα αίτια της εγκληματικής ενέργειας.
- Γίνεται σύνδεση των συμβάντων-αποδεικτικών στοιχείων με τους πιθανούς δράστες.
- Ελαχιστοποιούνται οι επιπτώσεις της επίθεσης έτσι ώστε να συνεχισθεί η εύρυθμη λειτουργία των επιχειρησιακών διαδικασιών.
- Τελευταίος στόχος είναι η επιτυχής έρευνα του περιστατικού.

Η δραστική ψηφιακή εγκληματολογία(Reactive Digital Forensics), περιλαμβάνει έξι φάσεις κατά τις οποίες εφαρμόζονται τεχνικές για την διαφύλαξη, ταυτοποίηση, την εξόρυξη, την τεκμηρίωση, την ανάλυση και τέλος την ερμηνεία των ψηφιακών μέσων, τα οποία αποθηκεύονται στην ψηφιακή τους μορφή και αποτελούν αποδεικτικά στοιχεία με σκοπό την διευκόλυνση και την ανασυγκρότηση των ψηφιακών πειστηρίων της επίθεσης.

Οι έξι φάσεις που εντάσσονται στην δραστική ψηφιακή εγκληματολογία είναι οι εξής:

Πρώτη φάση: Στο αρχικό στάδιο γίνεται αντιμετώπιση του περιστατικού και η επιβεβαίωση ότι το πληροφοριακό σύστημα έχει δεχτεί ψηφιακή επίθεση. Η φάση αυτή περιλαμβάνει τα ακόλουθα βήματα: την ανίχνευση του συμβάντος, την αναφορά του περιστατικού, την επιβεβαίωση του, την διατύπωση της υπόθεσης για το τι έχει συμβεί, χορήγηση άδειας για περαιτέρω έρευνα, καθορίζεται η στρατηγική «περιορισμού»-«απομόνωσης» του περιβάλλοντος του πληροφοριακού συστήματος που δέχθηκε την επίθεση , διαμορφώνεται το πλάνο της έρευνας, κατανέμονται οι πόροι για την διεξαγωγή της έρευνας και τέλος γίνεται η κοινοποίηση της διαδικασίας του ελέγχου.

Δεύτερη φάση: Στην δεύτερη φάση της δραστικής ψηφιακής εγκληματολογίας γίνεται, αν αυτό κριθεί απαραίτητο, φυσική έρευνα του περιβάλλοντος. Πολλές φορές κρίνεται απαραίτητο σε μια ψηφιακή έρευνα να συμπεριληφθεί φυσική εγκληματολογική έρευνα έτσι ώστε να συλλεχθούν όσο περισσότερα στοιχεία έτσι ώστε να εξασφαλίσουν μια επιτυχή διερεύνηση του εγκλήματος. Τα βήματα που ακολουθούνται είναι τα εξής: εξασφάλιση του φυσικού περιβάλλοντος που έλαβε χώρα η εγκληματική ενέργεια, έρευνα στο τόπο του εγκλήματος για πιθανά αποδεικτικά στοιχεία, αναζήτηση και συλλογή πειστηρίων, τεκμηρίωση των αποδεικτικών στοιχείων, συλλογή και ανάλυση των στοιχείων αυτών, εντοπισμό πιθανών ψηφιακών ενδείξεων, ανακατασκευή των γεγονότων, διατύπωση πορίσματος σύμφωνα με τα πειστήρια που συλλέχθηκαν και τέλος η μεταφορά και η αποθήκευση των αποδεικτικών στοιχείων.

Τρίτη φάση: Η Τρίτη φάση αναφέρεται στην ψηφιακή έρευνα της επίθεσης. Για μια επιτυχή ψηφιακή διερεύνηση ακολουθούνται τα εξής τρία βήματα:

1. Στο πρώτο βήμα γίνεται ο εντοπισμός και η συλλογή των αποδεικτικών στοιχείων. Στη συνέχεια αν τα αποδεικτικά στοιχεία αποτελούν «ζωντανές» αποδείξεις, ενεργοποιούνται οι διαδικασίες της ενεργής ψηφιακής εγκληματολογίας (Active Digital Forensics) που θα περιγραφούν σε επόμενη ενότητα. Στα επόμενα υπό-βήματα διασφαλίζεται η ακεραιότητα των πειστηρίων, η ταυτοποίηση τους, γίνεται μεταφορά και αποθήκευση των αποδεικτικών στοιχείων και τέλος τεκμηριώνεται η διαδικασία ανάκτησης τους.

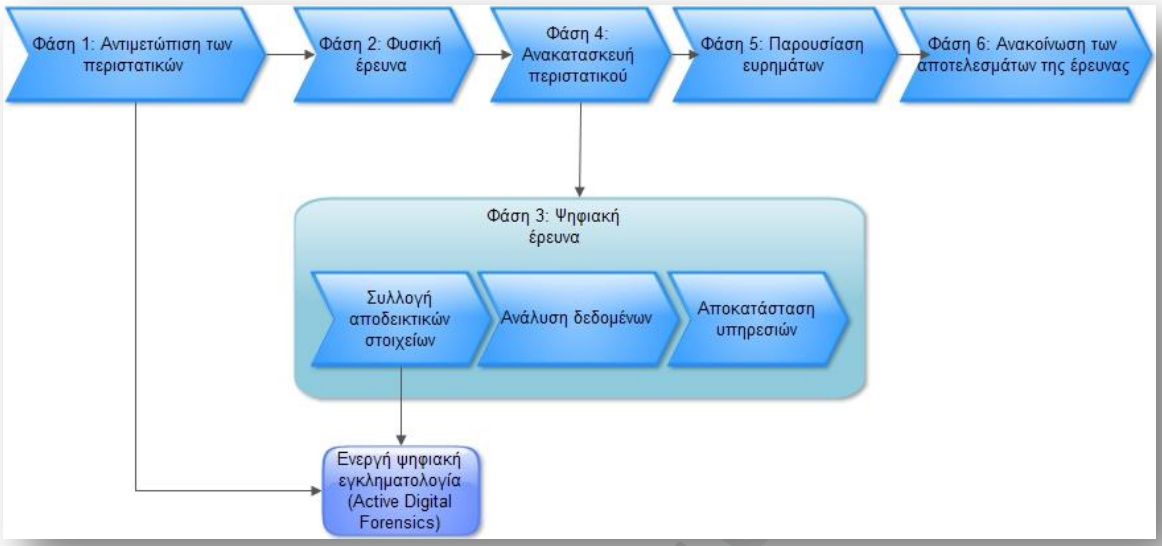
2. Το δεύτερο βήμα είναι αυτό της ανάλυσης των δεδομένων. Η ερευνητική ομάδα επανεξετάζει το σχέδιο έρευνας, αξιολογεί τα εργαλεία που είναι διαθέσιμα, διατυπώνει ένα υποθετικό σενάριο το οποίο στη συνέχεια εφαρμόζεται δοκιμαστικά με στόχο την ανακατασκευή της επίθεσης που δέχθηκε το πληροφοριακό σύστημα. Τέλος επικυρώνονται τα αποτελέσματα της ανάλυσης και διατυπώνονται σε έγγραφη μορφή.
3. Στο τρίτο και τελευταίο βήμα, επιχειρείται η αποκατάσταση των υπηρεσιών. Κατά την διάρκεια αυτού του βήματος γίνεται η αποκατάσταση των συστημάτων και των υπηρεσιών όσο το δυνατόν γρηγορότερα· εφόσον κριθεί απαραίτητο οι ερευνητές έρχονται σε συνεννόηση με την ομάδα διαχείρισης κινδύνων(risk management) του οργανισμού για την ασφαλή αποκατάσταση των υπηρεσιών και της συνέχειας των εργασιών της εταιρείας το συντομότερο δυνατόν.

Τέταρτη φάση: Κατά την διάρκεια αυτής της φάσης η ομάδα έρευνας παγιώνει τα αποτελέσματα της φυσικής έρευνας (δεύτερη φάση) και της ψηφιακής έρευνας (τρίτη φάση). Στην περίπτωση που τα ευρήματα δεν επαρκούν για υποστηρίξουν την υπόθεση τότε επαναλαμβάνονται η φάσεις δύο και τρία. Στο τέλος της τέταρτης φάσης οι ειδικοί ερευνητές παραθέτουν μια τεκμηριωμένη έκθεση με τις ψηφιακές αποδείξεις της έρευνας που υποστηρίζουν την υπόθεση.

Πέμπτη φάση: Η Πέμπτη φάση περιλαμβάνει την παρουσίαση των ευρημάτων, των προηγούμενων φάσεων, στις αρχές. Η ομάδα των ερευνητών θα προετοιμάσει την υπόθεση λαμβάνοντας υπόψη τις νομικές απαιτήσεις, συμπεριλαμβάνει το χρονοδιάγραμμα όλης της υπόθεσης και τέλος παρουσιάζει τα στοιχεία που περιγράφουν την υπόθεση.

Έκτη φάση: Στην τελευταία φάση της δραστικής ψηφιακής εγκληματολογίας, γίνεται η ανακοίνωση των αποτελεσμάτων της έρευνας και το κλείσιμο της υπόθεσης.

Το μοντέλο της δραστικής ψηφιακής εγκληματολογίας(Reactive Digital Forensics), μπορεί να παρομοιαστεί σαν ένα μοντέλο καταρράκτη όπου σε ορισμένα σημεία οι διάφορες φάσεις επαναλαμβάνονται (εφόσον αυτό κριθεί απαραίτητο κατά την διάρκεια μιας έρευνας). Στην εικόνα Εικόνα 11. Δραστική ψηφιακή εγκληματολογία (Reactive Digital Forensics)Εικόνα 11παρουσιάζονται οι φάσεις της δραστικής ψηφιακής εγκληματολογίας(Reactive Digital Forensics) . Η δραστική ψηφιακή εγκληματολογία διερευνά τα περιστατικά επιθέσεων , καθορίζει την ρίζα του συμβάντος και την επιτυχή δίωξη των δραστών.



Εικόνα 11. Δραστική ψηφιακή εγκληματολογία (Reactive Digital Forensics)

3.1.2.3 Ενεργή Ψηφιακή Εγκληματολογία (Active Digital Forensics)

Οι παραδοσιακές μέθοδοι της δραστικής ψηφιακής εγκληματολογίας μπορούν να εξασφαλίσουν μόνο ότι δεν θα γίνουν αλλαγές στα στοιχεία και τα δεδομένα που συλλέχθηκαν κατά την διάρκεια της έρευνας. Στην ενεργή ψηφιακή εγκληματολογία (Active Digital Forensics) οι ειδικοί ερευνητές χρησιμοποιούν κατάλληλα εργαλεία λογισμικού που καθιστούν αναπόφευκτες τις τυχόν αλλαγές σε δεδομένα που συλλέγονται. Είναι σημαντικό να τεκμηριώνεται η «ζωντανή» ερευνητική διαδικασία σύμφωνα με τις Δικανικές μεθόδους, έτσι ώστε τα στοιχεία που θα συλλεχθούν να γίνουν αποδεκτά σε μια Δικαστική αίθουσα. Οι εγκληματολόγοι της ενεργής ψηφιακής εγκληματολογίας κάνουν χρήση απομακρυσμένων εργαλείων της Δικανικής Πληροφορικής έτσι ώστε να διατηρούν και να αποκτούν τα επιθυμητά δεδομένα. Τα εργαλεία αυτά χρησιμοποιούν «ζωντανές» τεχνικές ανάλυσης οι οποίες χρησιμοποιούν το προϋπάρχων λογισμικό ενός πληροφοριακού συστήματος για να αντλήσουν τα απαραίτητα στοιχεία κατά την διάρκεια μιας έρευνας. Τα μηχανήματα ενός πληροφοριακού περιβάλλοντος που αποτελούν πιθανούς στόχους μιας επίθεσης παρακολουθούνται από τα Δικανικά εργαλεία, με στόχο να ανακτηθούν τα απαραίτητα δεδομένα για την προέλευση της πιθανής ψηφιακής επίθεσης. Στην ενεργή ψηφιακή εγκληματολογία (Active Digital Forensics) χρησιμοποιούνται ακόμα Δικανικά δικτυακά εργαλεία για τον εντοπισμό των πηγών «ζωντανών» αποδείξεων σε ένα δίκτυο. Πολλές φορές, επειδή δεν είναι δυνατόν να καταγράφονται όλες οι δραστηριότητες μέσα σε ένα δίκτυο ενός οργανισμού, χρησιμοποιούνται εργαλεία όπως DNS και Whois lookup & IP servers για τον εντοπισμό των πηγών της επίθεσης, παίρνοντας τις επιθυμητές πληροφορίες συμπληρώνοντας για παράδειγμα την IP κατέγραψε την στιγμή της επίθεσης ένα IDS σύστημα (αναλυτικότερη περιγραφή τέτοιων εργαλείων περιγράφονται στην Πειραματική ενότητα). Στην περίπτωση μιας ψηφιακής επίθεσης, το σύστημα ανίχνευσης εισβολών (IDS) ενός οργανισμού ανιχνεύει και ενεργοποιεί το Incident Response (IR) πρωτόκολλο (12). Το Incident Response (IR) πρωτόκολλο είναι ένα σχέδιο προσέγγισης για την αντιμετώπιση και τη διαχείριση των συνεπειών της παραβίασης της ασφάλειας ενός πληροφοριακού συστήματος. Στόχος είναι να υπάρχει διαχείριση της κατάστασης με έναν τρόπο που περιορίζει τις βλάβες στα πληροφοριακά συστήματα του οργανισμού και να

μειώνει το χρόνο και το κόστος ανάκτησης των υπηρεσιών. Ένα Incident Response (IR) πρωτόκολλο περιλαμβάνει μια πολιτική που καθορίζει συγκεκριμένα, το τι συνιστάται σε ένα συμβάν επιθέσεως και παρέχει μια βήμα προς βήμα διαδικασία που πρέπει να ακολουθείται όταν ενεργοποιηθεί ένα τέτοιο συμβάν. Υπάρχουν έξι βήματα για το χειρισμό ενός περιστατικού: προετοιμασία του πληροφοριακού συστήματος (μέτρα ασφαλείας), αναγνώριση ενός συμβάντος επίθεσης, απολογισμό για το ποια συστήματα έχουν υποστεί βλάβες και πρέπει να περιοριστούν για έρευνα, έρευνα για την προέλευση του περιστατικού, ανάκτηση των δεδομένων και των υπηρεσιών και τέλος ανάλυση του περιστατικού για να ληφθούν μέτρα ασφαλείας που θα προλαμβάνει όμοιες επιθέσεις. Παρόλα αυτά, καθίσταται αναγκαίο να ενσωματωθούν «ζωντανά» Δικανικά πρωτόκολλα (live forensic investigation protocols), με το πρωτόκολλο IR για να εξασφαλιστεί ότι θα είναι διαθέσιμα αποδεκτά ψηφιακά πειστήρια, αν αυτά απατηθούν για ερευνητικούς σκοπούς.

Για να συγκεντρωθούν «ζωντανά» στοιχεία από συστήματα όπως εικονικές μηχανές (virtual machines), πτητικούς δίσκους(volatile disks), pseudo files και στοιχεία όταν ένα σύστημα πέφτει σε λειτουργία αδρανοποίησης (hibernate mode) και δεδομένα που μεταβάλλονται μέσα σε ένα πληροφοριακό περιβάλλον, χρησιμοποιούνται υλικό- λογισμικές τεχνικές που επιτρέπουν την σύλληψη δεδομένων σε πραγματικό χρόνο. Χαρακτηριστικό παράδειγμα αποτελεί η μελέτη του B.Carrier (13) , σύμφωνα με την οποία γίνεται χρήση μιας PCI[8] κάρτας η οποία επιβλέπει ένα πληροφοριακό σύστημα, όπως για παράδειγμα πτητικούς δίσκους, virtual machines, επίβλεψη υπολογιστή σε κατάσταση αδρανοποίησης). Η μέθοδος αυτή αποδεικνύεται αποτελεσματική αλλά αρκετά δαπανηρή, ειδικά σε μεγάλα πληροφοριακά συστήματα, καθώς κάθε εξυπηρετητής(server) θα πρέπει να εφοδιάζεται με μια PCI κάρτα, για να επιτυγχάνεται η επίβλεψη του.

Η ενεργή ψηφιακή εγκληματολογία (Active Digital Forensics), είναι η ικανότητα ενός οργανισμού να συγκεντρώνει (εντοπισμό, τη συλλογή και τη διατήρηση), αποδεκτών ψηφιακών πειστηρίων σε ένα «ζωντανό» περιβάλλον έτσι ώστε να διευκολύνει μια επικείμενη Δικανική έρευνα. Αναλυτικότερά, οι στόχοι της ενεργής ψηφιακής εγκληματολογίας είναι η εξής:

- Η συλλογή σχετικών «ζωντανών» ψηφιακών πειστηρίων (συμπεριλαμβανομένων των πτητικών αποδείξεων), σε ένα ζωντανό περιβάλλον με την χρήση κατάλληλων εργαλείων και τεχνολογιών.
- Την ελαχιστοποίηση των επιπτώσεων στη λειτουργία των πληροφοριακών συστημάτων του οργανισμού σε ένα εν εξελίξει περιστατικό.
- Τελευταίος στόχος της ενεργής ψηφιακής εγκληματολογίας, είναι να παρέχεται ένα σημείο εκκίνησης για μια δραστική έρευνα εντός των παραμέτρων του πλαισίου ελέγχου κινδύνων του οργανισμού.

Στη συνέχεια γίνεται αναλυτική περιγραφή των τεσσάρων φάσεων που απαρτίζουν την ενεργή ψηφιακή εγκληματολογία.

Πρώτη φάση: Όπως έχει περιγραφεί και στην διαδικασία της δραστικής ψηφιακής εγκληματολογίας εκτελούνται τα ίδια βήματα με την διαφορά ότι θα πρέπει να καθοριστεί από τους ερευνητές ποια πτητικά ή «ζωντανά» στοιχεία θα πρέπει να ανακτηθούν για να εξασφαλισθεί μια επιτυχής έρευνα. Αν οι πολιτικές διαχείρισης κινδύνου επιτρέπουν να συνεχιστεί η έρευνα για την συλλογή πειστηρίων σύμφωνα με τις μεθόδους της ενεργής ψηφιακής εγκληματολογίας (Active Digital Forensics), διατυπώνεται το σχέδιο έρευνας, σε αντίθετη περίπτωση ξεκινάει η

[8] Ορισμός κάρτας PCI : http://en.wikipedia.org/wiki/Conventional_PCI

διαδικασία της δραστικής ψηφιακής εγκληματολογίας (Reactive Digital Forensics) όπως έχει περιγραφεί σχηματικά στην (Εικόνα 11). Επιπροσθέτως, θα πρέπει να προκαθοριστούν γεγονότα ενεργοποίησης τα οποία θα εκκινούν, σε ένα πληροφοριακό σύστημα, την ενεργό παρακολούθηση ή άλλες διαδικασίες, όταν μια προειδοποίηση συμβάντος ενεργοποιείται.

Δεύτερη φάση: Στην δεύτερη φάση γίνεται εκκίνηση της έρευνας η οποία διαιρείται σε δύο υπό-φάσεις:

1. Στο πρώτο βήμα, όπως συμβαίνει και στη φάση τρία της δραστικής ψηφιακής εγκληματολογίας, γίνεται συλλογή των «ζωντανών» αποδεικτικών στοιχείων, κάνοντας χρήση των κατάλληλων εργαλείων ή τεχνολογιών που θα βοηθήσουν σε περαιτέρω ανίχνευση του προφίλ του επιτιθέμενου ή θα αποκαλύψουν την πηγή της επίθεσης.

   Όλα τα δεδομένα που εξάγονται αποθηκεύονται και ασφαλίζονται μετά την διαδικασία της συλλογής, με στόχο να διατηρηθούν ακέραια μέχρι να αναλυθούν. Θεωρείται απαραίτητο να καταγράφονται όλες οι ενέργειες που εκτελούνται για να εξασφαλισθεί ότι τα αποκτηθέντα στοιχεία διατηρήθηκαν ακέραια.

   Θεωρείται απαραίτητο όλα τα εργαλεία ή εφαρμογές που έχουν ενσωματωθεί στο πληροφοριακό σύστημα του οργανισμού για την συλλογή των πειστηρίων, να ενεργοποιούνται αυτόματα το συντομότερο δυνατό όταν ανιχνευθεί κάποια επίθεση έτσι ώστε να συλλεχθούν αξιόπιστα στοιχεία. Τα εργαλεία αυτά θα πρέπει να λειτουργούν αυτόνομα και με όσο λιγότερη ανθρώπινη παρέμβαση. Επίσης θα πρέπει να εξασφαλίζεται η ελάχιστη τροποποίηση των στατικών ψηφιακών στοιχείων και η αντιγραφή ή εξαγωγή των δεδομένων θα πρέπει να γίνεται μόνο όταν αρχικά τα δεδομένα και timestamp[9] δεδομένα δεν έχουν επηρεαστεί.
2. Το δεύτερο βήμα περιλαμβάνει την ανάλυση των δεδομένων, όπως έχει περιγραφεί και στο φάση τρία της δραστικής ψηφιακής εγκληματολογίας (Reactive Digital Forensics). Τα αρχικά στοιχεία αναλύονται και προσδιορίζεται αν αποτελούν επαρκή αποδεικτικά στοιχεία έτσι ώστε να ανακατασκευαστεί το συμβάν της επίθεσης και να υποστηρίξει την αρχική υπόθεση. Όλες οι διαδικασίες της ενεργής ψηφιακής εγκληματολογίας θα πρέπει να τεκμηριώνονται σε κάθε βήμα για τη διασφάλιση της ακεραιότητας όλων των αποδεικτικών στοιχείων κατά την διάρκεια της έρευνας. Θα πρέπει να ληφθεί υπόψη, καθ' όλη την διάρκεια της έρευνας, η διατήρηση της αξιοπιστίας και το αποδεκτό των αποτελεσμάτων.

Τρίτη φάση: Στην εν λόγω φάση χρησιμοποιούνται τα αποτελέσματα από την φάση της ανάλυσης (φάση δύο βήμα 2^{ο}), έτσι ώστε να επιτευχθεί η ανακατασκευή του συμβάντος της επίθεσης. Στη συνέχεια θα πρέπει να καθοριστεί αν τα «ζωντανά» αποδεικτικά στοιχεία που έχουν συλλεχθεί επαρκούν για σταματήσει η ψηφιακή εγκληματολογική έρευνα. Στην αντίθετη περίπτωση, που τα στοιχεία δεν επαρκούν ή δεν μπορούν να γίνουν αποδεκτά επαναλαμβάνεται η δεύτερη φάση της μεθόδου. Το πλαίσιο διαχείρισης κινδύνων (Risk management framework), θα καθορίσει αν τελικά η έρευνα πρέπει να τερματιστεί η διαδικασία σύμφωνα με τις προϋποθέσεις που ορίζει αυτό, για παράδειγμα ο επαρκής αριθμός ψηφιακών πειστηρίων που συλλέχθηκαν ή το κόστος τις έρευνας ξεπερνάει το ανώτερο επιτρεπτό.

[9] Ορισμός timestamp : http://en.wikipedia.org/wiki/Timestamp

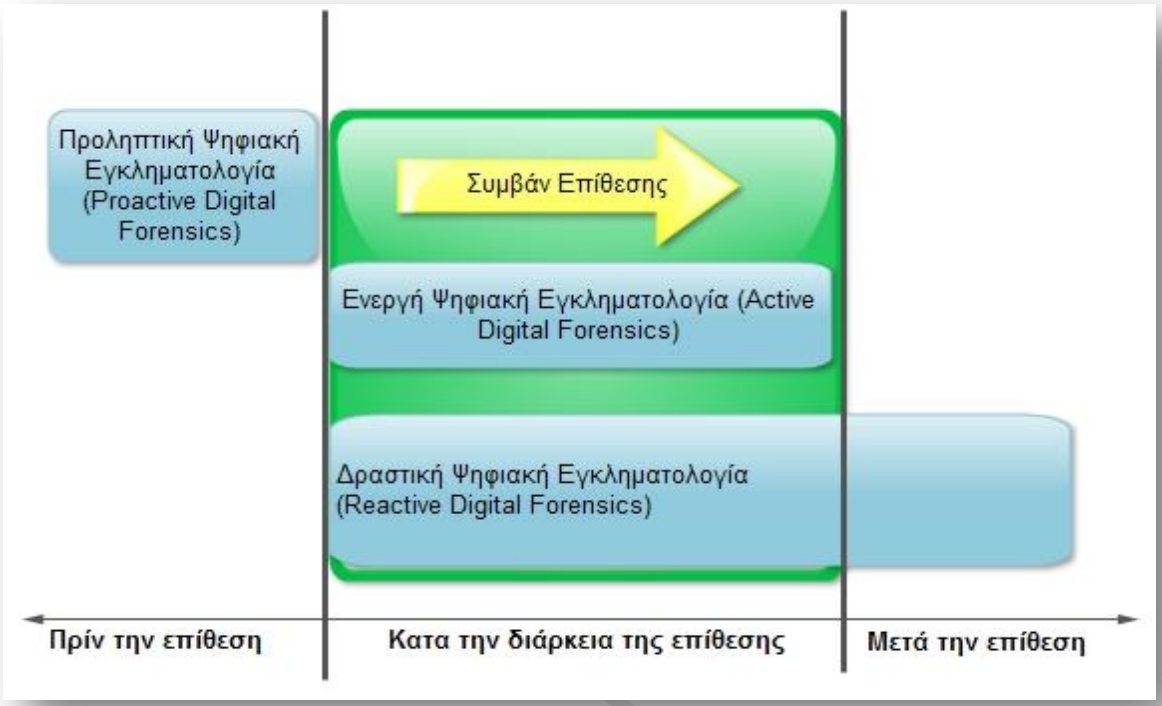
Τέταρτη φάση: Στην τελευταία φάση και εφόσον έχουν συγκεντρωθεί επαρκή αποδεικτικά στοιχεία, οι ειδικοί ερευνητές προετοιμάζουν τεκμηριωμένα έγγραφα της υπόθεσης με σκοπό να συνεχίσει η ομάδα της δραστικής ψηφιακής έρευνας και να ολοκληρωθεί η διερεύνηση του συμβάντος. Μετά την ολοκλήρωση της ενεργής ψηφιακής έρευνας, με τις μεθόδους της δραστικής ψηφιακής έρευνα αναλύονται και ανακατασκευάζονται τα περιστατικά της επιθέσεως με όλα τα αποδεικτικά στοιχεία, συμπεριλαμβανομένων και των πειστηρίων που μπορεί να προέκυψαν από την φυσική έρευνα, που απαιτούνται για να ολοκληρωθεί επιτυχώς η εγκληματολογική διερεύνηση.

Συνοψίζοντας το αντικείμενο της ενεργής ψηφιακής εγκληματολογίας (Active Digital Forensics), προσανατολίζεται στο να συγκεντρωθούν «ζωντανά» αποδεικτικά στοιχεία κατά την διάρκεια των επιθέσεων. Στο σχήμα, (Εικόνα 12), που ακολουθεί δίνεται διαγραμματικά η διαδικασία των φάσεων της ενεργής ψηφιακής εγκληματολογίας.

Εικόνα 12. Ενεργή ψηφιακή εγκληματολογία (Active Digital Forensics)

3.1.2.4 Σχέσεις μεταξύ των Αντικειμένων

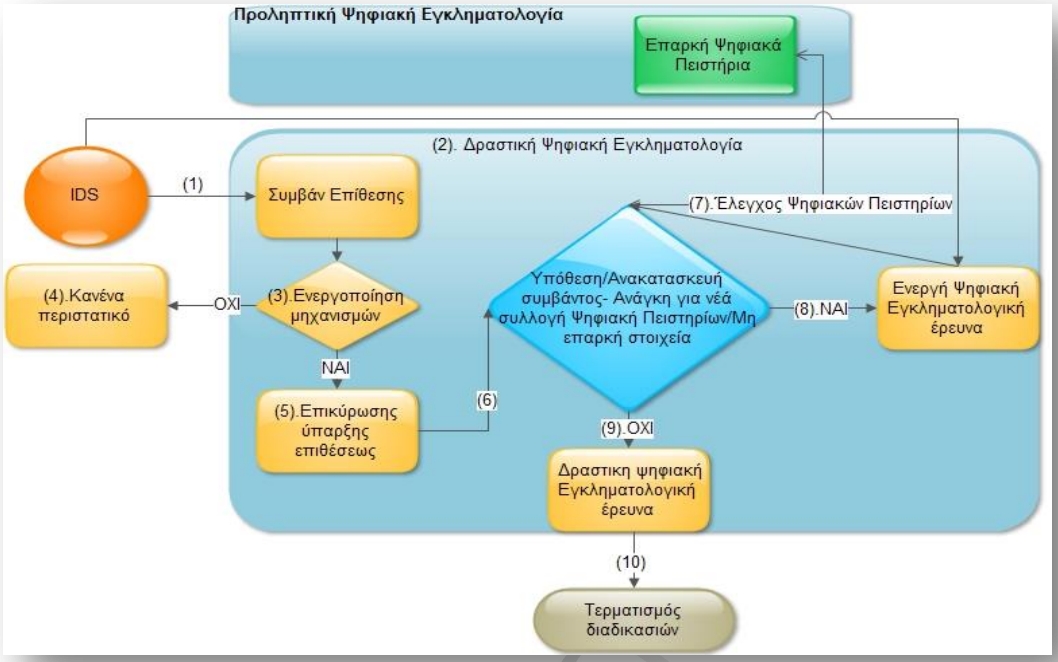
Στη συγκεκριμένη ενότητα θα δοθεί σύντομο παράδειγμα για να γίνει κατανοητή η συσχέτιση των τριών αντικειμένων που περιγράφηκαν στις προηγούμενες ενότητες. Το σχήμα στην Εικόνα 13. Αντικείμενα της Ψηφιακής Εγκληματολογίας, μας δίνει διαγραμματική περιγραφή των τριών μεθοδολογιών .



Εικόνα 13. Αντικείμενα της Ψηφιακής Εγκληματολογίας

Από το σχήμα παρατηρούμε ότι αρχικά και πριν την επίθεση, σε ένα οργανισμό έχουν εφαρμοσθεί όλες οι μέθοδοι και τα εργαλεία της προληπτικής ψηφιακής Εγκληματολογίας, όπως για παράδειγμα ένα σύστημα IDS. Κατά την διάρκεια της επίθεσης, ενεργοποιούνται ανάλογα με το είδος του συμβάντος και ποια σημεία του πληροφοριακού συστήματος δέχθηκαν την επίθεση, οι διαδικασίες της ενεργής ψηφιακής εγκληματολογίας είτε οι διαδικασίες της δραστικής ψηφιακής εγκληματολογίας είτε και οι δύο αν αυτό κριθεί απαραίτητο. Μετά το τέλος της επίθεσης, μπορούν να μπουν σε εφαρμογή μόνο οι διαδικασίες της δραστικής ψηφιακής εγκληματολογίας καθώς είναι δυνατό να συλλεχθούν πειστήρια που αφορούν μόνο την μη «ενεργή» εγκληματολογία (“dead” forensics).

Στην εν λόγω παράγραφο δίνεται ένα σύντομο παράδειγμα λειτουργίας και των σχέσεων μεταξύ των τριών αντικειμένων της ψηφιακής εγκληματολογίας. Στο σχήμα (Εικόνα 14) παρουσιάζεται η σχέση των τριών αντικειμένων της ψηφιακής εγκληματολογίας (Digital Forensics), κατά την διάρκεια όλων των φάσεων μιας επικείμενης επίθεσης.



Εικόνα 14. Σχέσεις μεταξύ των Ψηφιακών Εγκληματολογικών αντικειμένων

Όπως παρατηρείται και στην (Εικόνα 14), στο πληροφοριακό περιβάλλον ενσωματώνεται σύστημα ανίχνευσης εισβολών (IDS). Στο αρχικό στάδιο και μετά από την ύπαρξη ενός συμβάντος (βήμα 1), που ανιχνεύεται από το IDS σύστημα, γίνεται λήψη της απόφασης αν θα πρέπει να ενεργοποιηθούν οι μηχανισμοί της ψηφιακής έρευνας (βήμα 3), έτσι ώστε να συλλεχθούν τα απαραίτητα στοιχεία ανάλογα με το είδος της εγκληματολογικής εξέτασης που θα ακολουθήσει· είτε δραστικής ή ενεργής όπως φαίνονται στα βήματα (2) και (8). Αν δεν έχει καταγραφεί κάποιο συμβάν επιθέσεως, δεν εκτελείται καμία διαδικασία (βήμα 4), σε αντίθετη περίπτωση γίνεται επικύρωση για την ύπαρξη επιθέσεως όπως αυτό φαίνεται στο βήμα (5). Στο βήμα (6) γίνονται υποθέσεις για τι συμβάν έγινε, σε ποιο σημείο του οργανισμού, με ποιόν τρόπο και ποια χρονική στιγμή, επίσης ξεκινάει η διαδικασία ανακατασκευής του συμβάντος της επίθεσης. Στη συνέχεια γίνεται έλεγχος αν τα «ζωντανά» πειστήρια της ενεργής ψηφιακής εγκληματολογικής έρευνας στο βήμα (8) που συλλέχθηκαν επαρκούν (έλεγχος στο βήμα 7- παρατηρείται ότι η σχέση είναι αμφίδρομη), η διαδικασία συνεχίζεται στο βήμα (9) με την δραστική ψηφιακή εγκληματολογική έρευνα. Σε αντίθετη περίπτωση τα βήματα (8) και (9) για την συλλογή «ζωντανών» ή μη ενεργών πειστηρίων, επαναλαμβάνονται. Όταν ολοκληρωθεί και η συλλογή των μη ενεργών δεδομένων η διαδικασία τερματίζεται στο βήμα (10).

Συνοψίζοντας, η προληπτική ψηφιακή εγκληματολογία είναι υπεύθυνη για την χρήση όλων των εργαλείων και των τεχνικών που θα διευκολύνουν μια δικανική έρευνα και θα απλοποιήσουν την συλλογή των πειστηρίων που θα παρουσιαστούν στις Δικαστικές αρχές. Η δραστική ψηφιακή εγκληματολογία χρησιμοποιείται για να προσδιοριστεί η ρίζα του προβλήματος και η ανακατασκευή του συμβάντος. Τέλος, η ενεργή ψηφιακή εγκληματολογική έρευνα αφορά όλες τις διαδικασίες για την συλλογή «ζωντανών» αποδεικτικών στοιχείων σε πραγματικό χρόνο ή σε «ζωντανά» περιβάλλοντα κατά την διάρκεια των επιθέσεων.

3.1.3 Μεθοδολογία στα Web Services

Οι υπηρεσίες ιστού (web services) χρησιμοποιούνται για εμπορικούς, στρατιωτικούς, κυβερνητικούς λόγους. Νέες υπηρεσίες ιστού μπορούν να δημιουργηθούν και να περιέχουν ή να συνεργάζονται με υπάρχοντα web services χρησιμοποιώντας τεχνικές όπως της ενορχήστρωσης (orchestration[10] ή Enterprise integration Application[11]) και η χορογραφία υπηρεσιών ιστού (Web Services choreography[12]).

Η ενορχήστρωση (Web Service orchestration) επιτρέπει σε επίπεδο πλατφόρμας (platform layer) την σύνθεση και τον συνδυασμό διαφόρων υπηρεσιών ιστού σε συνεχείς συναλλαγές (transactions) σε ένα περιβάλλον επιχειρηματικών διαδικασιών.

Η χορογραφία υπηρεσιών ιστού (Web Services choreography) αναφέρεται στις προδιαγραφές για το πώς τα μηνύματα θα πρέπει να «ρέουν» μεταξύ των διαφόρων υπηρεσιών, χρησιμοποιώντας διασυνδεδεμένα στοιχεία και εφαρμογές για να διασφαλίσουν την βέλτιστη διαλειτουργικότητα.

Οι παραπάνω τεχνικές δημιουργούν σε επίπεδο υπηρεσιών σύνθετες αλληλοσυσχετίσεις μεταξύ των υπηρεσιών ιστού διαφορετικών οργανισμών. Παρόλα αυτά, οι διαφορετικές «συνθέσεις» μεταξύ των υπηρεσιών δημιουργούν υπηρεσίες αλληλεξαρτήσεων οι οποίες μπορούν να χρησιμοποιηθούν για κακόβουλη χρήση και για μη νόμιμους σκοπούς. Κατά την διάρκεια λειτουργίας των υπηρεσιών Ιστού (Web Services), πολλοί εξυπηρετητές και οργανισμοί επηρεάζονται και πολλές φορές αποφέρουν οικονομικές απώλειες και βλάβες στην υποδομή μιας επιχείρησης.

Για την αποτελεσματική διερεύνηση ενός κακόβουλου γεγονότος σε ένα σύνολο υπηρεσιών ιστού, προϋποθέτει τα αιτήματα μεταξύ των υπηρεσιών να «εκτελούνται» με ένα ουδέτερο και ασφαλή τρόπο έτσι ώστε η φερόμενη δραστηριότητα τους να αναδημιουργηθεί που θα διασφαλίσουν τα αποδεικτικά στοιχεία τα οποία θα οδηγήσουν και θα υποστηρίξουν μια ενδεχόμενη ποινική δίωξη. Όταν μια κακόβουλη χρήση των υπηρεσιών ιστού ανιχνευτεί, οι ερευνητές του ηλεκτρονικού εγκλήματος θα πρέπει να συλλέξουν τα κατάλληλα αρχεία καταγραφής (log files) έτσι ώστε να ανακατασκευάσουν το συμβάν το οποίο συνέβη κατά την αλληλεπίδραση μεταξύ των υπηρεσιών ιστού και να εξάγουν σωστά πορίσματα. Τα αποδεικτικά στοιχεία που εξάγονται από εξυπηρετητές Ιστού (Web Servers), όπως XML[13] ειδοποιήσεις (alerts) του τείχους προστασίας (firewall) από το endpoint των υπηρεσιών και τα αρχεία καταγραφής(log records) του διακομιστή ιστού (Web Server), έχουν μικρή εγκληματολογική αξία. Σε μια ενδεχόμενη δίκη οι κατηγορούμενοι μπορούν να ισχυριστούν ότι δεν έστειλαν τα εν λόγω μηνύματα μέσω των υπηρεσιών ιστού ή ότι οι ενάγοντες άλλαξαν τα αρχεία καταγραφής έτσι ώστε να κατασκευάσουν τις υποθέσεις τους.

Την αντιμετώπιση αυτών των επιθέσεων καλείται να αντιμετωπίσει η Δικανική των υπηρεσιών ιστού (Forensic Web services), η οποία διαφυλάσσει τα αποδεικτικά στοιχεία που απαιτούνται για την ανακατασκευή μιας επιθέσεις που αποτελείται από την συνδυασμένη λειτουργία διαφόρων υπηρεσιών ιστού. Πρόβλημα αποτελεί ότι η Δικανικές υπηρεσίες ιστού δεν μπορούν να εξετάσουν ένα συμβάν επιθέσεως μεταξύ δύο ή περισσοτέρων web υπηρεσιών, μονομερώς καθώς λόγω των δυναμικών συνθέσεων και συνδυασμό αυτών.

[10] Ορισμός Web services orchestration: http://searchsoa.techtarget.com/answer/What-is-Web-services-orchestration
[11] Ορισμός EIA: http://en.wikipedia.org/wiki/Enterprise_application_integration
[12] Ορισμός Web services choreography: http://en.wikipedia.org/wiki/Web_Service_Choreography
[13] Ορισμός XML : http://www.w3.org/XML/

Για την αποτελεσματική αντιμετώπιση και διερεύνηση εγκληματικών επιθέσεων στο επίπεδό των υπηρεσιών ιστού, οι Δικανικές υπηρεσίες ιστού θα πρέπει να είναι ενσωματωμένες με τις υπηρεσίες ιστού που τις απαιτούν, οι υπηρεσίες που συνδυάζονται έτσι ώστε να δώσουν ένα επιθυμητό αποτέλεσμα ονομάζονται και «πελατειακές» web υπηρεσίες.

Η Εγκληματολογικές web υπηρεσίες[14] παρέχουν ένα κεντρικοποιημένο σημείο πρόσβασης στις υπηρεσίες «πελατών». Οι πληροφορίες που διατηρούνται από τις Δικανικές που παίζουν το ρόλο «τρίτων» έμπιστων οντοτήτων μεταξύ των υπολοίπων υπηρεσιών, παρέχονται στους ειδικούς εγκληματολόγους.

Οργανισμοί των οποίων οι λειτουργία είναι άρρητα συνδεμένη με την συνδυαστική λειτουργία διαφόρων web υπηρεσιών, μπορούν να επωφεληθούν από τις Δικανικές υπηρεσίες ιστού με πολλούς τρόπους. Ένα από τα οφέλη αυτής της μεθόδου είναι ότι οι Δικανικές υπηρεσίες ελέγχουν τις συνεργαζόμενες υπηρεσίες ιστού και λειτουργώντας ως ενδιάμεσος κόμβος «ελέγχουν» και καταγράφουν την λειτουργία τους όταν οι ευπάθειες αυτών επηρεάζουν την εμπιστευτικότητα και την διαθεσιμότητα της λειτουργίας τους(19) (20). Επίσης, οι λεπτομέρειες από μια κακόβουλη δραστηριότητα μπορεί να έχουν αντίκτυπο στα ποινικά μέτρα που πρέπει να ληφθούν και να επηρεάσουν την εξέλιξη μιας δικαστικής απόφασης.

3.1.3.1 Επιθέσεις Υπηρεσιών Ιστού

Οι επιθέσεις σε υπηρεσίες ιστού που εντοπίζονται στο διαδίκτυο είναι πολυάριθμες, μερικές από αυτές όπως WSDL/UDDI σάρωση, επιθέσεις επανάληψης, επανεγγραφή XML (XML rewriting), XSS (cross write scripting), υποκλοπή δεδομένων μεταξύ των υπηρεσιών (eavesdropping), επιθέσεις man in the middle, μπορούν να προκαλέσουν σοβαρές επιπτώσεις στην λειτουργία ενός οργανισμού ή και ακόμα οικονομικές απώλειες από την καταστροφή ή την υποκλοπή ευαίσθητων δεδομένων.

Για παράδειγμα μια επίθεση cross write scripting, μπορεί να υποκλέψει ευαίσθητα προσωπικά δεδομένα χρηστών μιας web υπηρεσίας. Το cross write scripting (XSS) επιτρέπει στον επιτιθέμενο να εκτελέσει κακόβουλο Javascript κώδικα στον φυλλομετρητή κάποιου χρήστη. Ο επιτιθέμενος δεν στοχεύει κατευθείαν κάποιον συγκεκριμένο χρήστη, αλλά εξαπολύει ένα κακόβουλο κώδικα σε ένα Ιστότοπο έτσι ώστε να καταστήσει τον συγκεκριμένο ιστότοπο ευπαθές για τους χρήστες που το επισκέπτονται. Στον φυλλομετρητή του χρήστη, ο κακόβουλους JavaScript κώδικας μοιάζει να είναι μέρος του Ιστότοπου με αποτέλεσμα να εκτελείται.

Ο μόνος τρόπος να εκτελεστεί ένα κακόβουλο κομμάτι κώδικα για ένα επιτιθέμενο στον φυλλομετρητή του θύματος, είναι να εισάγει τον επιθυμητό κώδικα σε μια από τις σελίδες που επισκέπτεται το θύμα. Εάν μια ιστοσελίδα περιέχει απευθείας εισαγωγή δεδομένων στις σελίδες της, σε αυτή την περίπτωση ο επιτιθέμενος μπορεί να εισάγει ένα «string» κώδικα που θα εκτελεστούν σαν «υγιές» κομμάτι κώδικα από τον φυλλομετρητή του χρήστη.

Συνάττονται τρείς τύποι XSS επιθέσεων:

- Η μη-επίμονη επίθεση (non-persistent attack). Είναι η πιο κοινή επίθεση, χρησιμοποιείται συνήθως σε τεχνικές phishing. Οι επιθέσεις προϋποθέτουν το «θύμα» να πατήσει πάνω στον κακόβουλο σύνδεσμο (URL) , για παράδειγμα σύνδεσμο που υποθετικά ο οποίος αναδρομολογεί το χρήστη σε μια μηχανή κοινωνικής δικτύωσης. Ο κακόβουλος κώδικας

[14] Οι Εγκληματολογικές υπηρεσίες ιστού αναφέρονται στο κείμενο και ως Δικανικές web υπηρεσίες.

μπορεί να «κρύβεται» σε ένα πεδίο φόρμας, ένα url ή ακόμα και σε ένα κρυφό πεδίο και συνήθως εσωκλείονται σε κώδικα της μορφής </script>… </script>. Με τις non-persistent επιθέσεις ένα κακόβουλος χρήστης μπορεί να υποκλέψει ευαίσθητα δεδομένα, να παραποιήσει τα δεδομένα ενός ιστοχώρου, να δημιουργήσει μια ψεύτικη ιστοσελίδα ή spam emails.

- Persistent (stored) XSS επιθέσεις. Οι Persistent XSS επιθέσεις είναι παρόμοιες με τις non-persistent με την διαφορά το κακόβουλο λογισμικό δεν εκτελείται σε κάποιον μεμονωμένο χρήστη, αλλά σε όλους τους επισκέπτες της «μολυσμένης» ιστοσελίδας. Αυτό συμβαίνει γιατί ο κακόβουλος κώδικας αποθηκεύεται στη βάση δεδομένων του website και φορτώνεται αυτόματα από τον κώδικα των ιστοσελίδων.
- Επιθέσεις τύπου DOM. Ο συγκεκριμένος τύπος επίθεσης XSS μπορεί να λειτουργήσει τοπικά έχοντας, ένας χρήστης, αποθηκεύσει μια ιστοσελίδα στον υπολογιστή του. Σε αντίθεση με τις προηγούμενες μεθόδους δεν χρειάζεται να αποθηκευτεί ο κακόβουλος κώδικας σε ένα εξυπηρετητή έτσι ώστε να επιστραφεί στον browser ενός θύματος αλλά ούτε στην βάση δεδομένων μιας ιστοσελίδας. Ο κακόβουλος κώδικας τοποθετείται στην σελίδα απόκρισης (response page), δηλαδή από την μεριά του πελάτη (client). Ο κώδικας που περιέχεται στη σελίδα από την μεριά του πελάτη, εκτελείται διαφορετικά λόγων των κακόβουλων τροποποιήσεων που έχουν περιέλθει στο περιβάλλον της γλώσσας DOM[15] (Document Object Model).

Με τις XSS επιθέσεις ένας επιτιθέμενος μπορεί να εισάγει κακόβουλο κώδικα σε μορφή Javascript, ActiveX ή HTML σε ευάλωτες εφαρμογές, κάνοντας εκμετάλλευση XSS ευπαθειών. Το πρόγραμμα περιήγησης επεξεργάζεται αυτόν τον κώδικα σαν να ήταν νόμιμο περιεχόμενο της ιστοσελίδας με τα αντίστοιχα δικαιώματα ασφαλείας, με αποτέλεσμα να καταστροφή των διαφόρων ρυθμίσεων μιας ιστοσελίδας και ευαίσθητών πληροφοριών των χρηστών.

Οι πιθανές XSS επιθέσεις που μπορούν να διαχωριστούν στις εξής κατηγορίες:

1. Υποκλοπή cookies. Τα cookies χρησιμοποιούνται για να διαχειρίζεται τις συνεδρίες ένα πρόγραμμα περιήγησής. Κάθε άτομο που συνδέεται σε μια ιστοσελίδα παίρνει ένα μοναδικό cookie το οποίο αποτελεί κλειδί για την ιστοσελίδα αυτή.
2. Phising. Κατά την διαδικασία του Phising οι κακόβουλοι χρήστες προσπαθούν να αποκτήσουν ευαίσθητες πληροφορίες όπως ονόματα χρηστών, κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών, έχοντας «μεταμφιεστεί» σαν αξιόπιστες οντότητες στο πλαίσιο μιας ηλεκτρονικής επικοινωνίας.
3. Πειρατεία λογαριασμών (Account Hijacking). Ο όρος αυτός αναφέρεται όταν ένα κακόβουλο λογισμικό - malware, εισχωρεί και εκτελείται σε ένα σύστημα ερχόμενο σε αντίθεση με τις κανονικές λειτουργίες του συστήματος που έχει προσβληθεί από τον κακόβουλο κώδικα.
4. Τέλος, η αλλαγή των ρυθμίσεων ενός χρήστη. Ο επιτιθέμενος θα μπορούσε να λάβει πληροφορίες σχετικά με τον διαχειριστή ενός ιστοτόπου προκειμένου να έχει πρόσβαση σε ευαίσθητα δεδομένα ή για να τροποποιήσει τις ρυθμίσεις των διάφορων χρηστών που τον επισκέπτονται.

[15] Η Document Object Model (DOM), είναι μια cross platform γλώσσα προγραμματισμού για την αναπαράσταση και την αλληλεπίδραση με τα αντικείμενα σε HTML , XHTML και XML έγγραφα.

3.1.3.2 Πλαίσιο Δικανικών web Υπηρεσιών

Το πλαίσιο των Δικανικών web υπηρεσιών αποτελείται από δύο υπηρεσίες. Η πρώτη υπηρεσία δημιουργεί αποδεικτικά στοιχεία από την συνδυαστική λειτουργία μεταξύ ζευγαριών web υπηρεσιών. Η δεύτερη υπηρεσία συνθέτει, μετά από αίτημα, αποδεικτικά στοιχεία τα οποία δημιουργούνται από την αλληλεπιδράσεις των διάφορων web υπηρεσιών και δημιουργεί ένα σύνθετο σενάριο που προκύπτει από την αλληλεπίδρασή των εν λόγω υπηρεσιών.

Στην συγκεκριμένη μεθοδολογία, αντιμετωπίζονται τρείς διαφορετικές προϋποθέσεις:

- Αξιόπιστες «τρίτες» οντότητες (trusted third parties) σε ένα ασφαλές και αξιόπιστο περιβάλλον.
  Θεωρείται απαραίτητο ότι τα Δικανικά δεδομένα συλλέγονται και επεξεργάζονται από μια ανεξάρτητη, «τρίτη» αρχή. Οι Δικανικές Υπηρεσίες ιστού θα πρέπει να τρέχει πάνω από ένα ασφαλές δικτυακό επίπεδο που παρέχει:
    1. Αυθεντικοποίηση όλων των οντοτήτων που λαμβάνουν χώρα.
    2. Εμπιστευτικότητα και αξιοπιστία των καναλιών επικοινωνίας.
    3. Αξιόπιστη ανταλλαγή μηνυμάτων πάνω από τα κανάλια επικοινωνίας.
- Ζεύγη αποδεικτικών στοιχείων καταγραφής με χρονοσήμανση.
  Η κύρια αρμοδιότητα των Δικανικών Web υπηρεσιών είναι η συλλογή αποδεικτικών στοιχείων της επικοινωνίας μεταξύ των ζευγών του εξυπηρετητή και του αιτούντα μιας web υπηρεσίας. Όλα τα αποδεικτικά στοιχεία κατά την διάρκεια των συναλλαγών που θα συλλέγονται από τις Δικανικές Webυπηρεσίες θα πρέπει να έχουν χρονοσήμανση και να περιλαμβάνουν:
    1. Χρόνος αίτησης της υπηρεσίας. Ο ακριβής χρόνος του ρολογιού του αιτούντα στέλνει μήνυμα στον εξυπηρετητή.
    2. Χρόνος ανταπόκρισης της υπηρεσίας. Η ακριβής ώρα που στέλνει απάντηση ο εξυπηρετητής στον αιτούντα.
    3. Λήξη της υπηρεσίας αιτήματος. Όταν μια Δικανική Web Υπηρεσία αποστέλλει επικυρωμένο μήνυμα ότι ο εξυπηρετητής απέτυχε να απαντήσει στην αίτημα σε ένα ορισμένο χρονικό διάστημα σύμφωνα με ρολόι του Δικανικού εξυπηρετητή.
    4. Χρόνος διαθεσιμότητας του εξυπηρετητή. Όταν μια Web Δικανική στέλνει πιστοποιημένο μήνυμα στον εξυπηρετητή για να ελέγξει την διαθεσιμότητα αυτού.

Τέλος, οι Δικανικές Υπηρεσίες ιστού σε σχέση με τους Δικανικούς εξυπηρετητές, συνθέτουν ένα ιστορικό «συναλλαγών» από την επικοινωνία πολλαπλών Web υπηρεσιών που πραγματοποιήθηκαν σε συγκεκριμένα χρονικά διαστήματα.

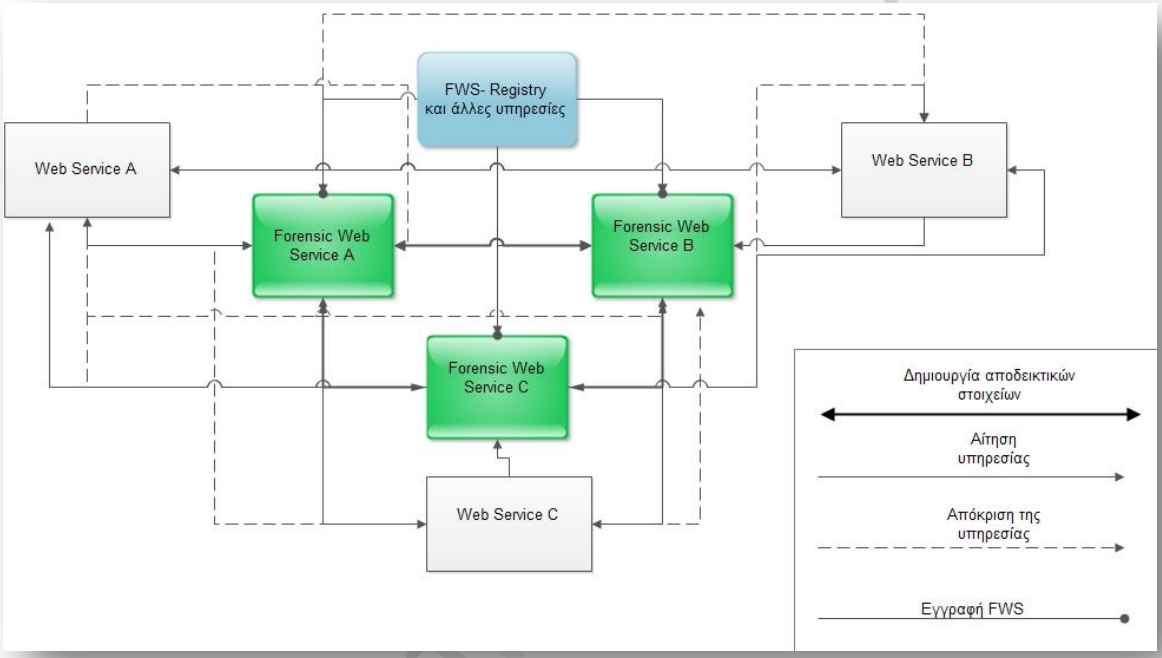
Το πλαίσιο των Δικανικών υπηρεσιών χρησιμοποιεί ενδιάμεσα στην λειτουργία των υπολοίπων web υπηρεσιών, αξιόπιστες «τρίτες» υπηρεσίες. Για την χρησιμοποίηση των Δικανικών υπηρεσιών θα πρέπει όλες οι υπηρεσίες ιστού να «υπογραφούν» από μια Δικανική web υπηρεσία και όλοι οι πράκτορες (agents[16]) των Δικανικών υπηρεσιών πρέπει να συνεργάζονται παρέχοντας αποδεικτικά στοιχεία σχετικά με τις συναλλαγές μεταξύ των web υπηρεσιών. Οι ρόλοι που εμπλέκονται στην διαδικασία είναι οι εξής τέσσερις:

1. Του αποστολέα του μηνύματος.
2. Του αποδέκτη.

[16] Agents : Υπολογιστικά προγράμματα τα οποία χρησιμοποιούν τεχνητή νοημοσύνη για να «εκπαιδευτούν» και να αυτοματοποιήσουν συγκεκριμένες διαδικασίες και διεργασίες.

3. Τον χειριστή των Δικανικών υπηρεσιών. Αναφέρεται στις web Δικανικές υπηρεσίες που επιλέγονται από τα δύο συμβαλλόμενα μέρη (αποστολέα- αποδέκτη).
4. Τέλος, ο χειριστής όλων των υπολοίπων web υπηρεσιών όπου δεν εμπλέκουν web Δικανικούς μηχανισμούς ή non-operator.

Παρακάτω παρουσιάζεται μια γραφική απεικόνιση του πλαισίου FWS (Δικανικών Web Υπηρεσιών).



Ένα μητρώο (registry), όπως παρουσιάζεται και στο παραπάνω σχήμα, είναι διαθέσιμο για την εύρεση όλων των διαθέσιμων καταχωρημένων web Δικανικών εξυπηρετητών. Τα συστήματα των Δικανικών web υπηρεσιών θα πρέπει να ικανοποιούν τις παρακάτω προϋποθέσεις:

- Η web υπηρεσία που ονομάζεται στοίβα (stack), θα πρέπει να «εμπλουτιστεί» με το επίπεδο των web Δικανικών υπηρεσιών. Η στοίβα αποτελείται από τρία επίπεδα: το κατώτατο επίπεδο αποτελείται από μηνύματα SOAP[17], το μεσαίο επίπεδο της στοίβας εμπεριέχει WS-Secure επικοινωνία (WS-SecureConversations)[18] και τέλος το ανώτερο επίπεδο αποτελείται από μηχανισμούς WSDL[19]. Το επίπεδο των Δικανικών υπηρεσιών προστίθεται μεταξύ του μεσαίου και ανώτερου επιπέδου της στοίβας με σκοπό να αναδρομολογήσει τις συναλλαγές μεταξύ των υπηρεσιών, μέσω των Δικανικών

[17] Τα SOAP μηνύματα είναι μονόδρομες μεταδόσεις από τον αποστολέα στο δέκτη, τα SOAP μηνύματα συχνά συνδυάζονται για την εισαγωγή μοτίβων όπως αιτήματος/απάντησης.
[18] Το WS – SecureConversations είναι μια υπηρεσία που παρέχει ασφαλή επικοινωνία μεταξύ των Web υπηρεσιών χρησιμοποιώντας session keys (http://searchsoftwarequality.techtarget.com/definition/WS-SecureConversation) .
[19] Το WSDL παρέχει λεπτομέρειες για τις τεχνικές προδιαγραφές μιας υπηρεσίας (http://searchsoa.techtarget.com/answer/WSDL-technology).

εξυπηρετητών. Η web υπηρεσία του αποστολέα και η αντίστοιχη του παραλήπτη επικοινωνούνε χρησιμοποιώντας το WSDL ανεξάρτητα από το επίπεδο του WS-Forensics (Δικανικών Web Υπηρεσιών).

- Μια συγκεκριμένη δομή μηνύματος απαιτείται έτσι ώστε να επιτευχθεί η επικοινωνία με WS-Forensics επίπεδο και την αποθήκευση των μηνυμάτων αυτών στους FWSs εξυπηρετητές.
  Τα WS-Forensics Μηνύματα έχουν την παρακάτω δομή:

```
1   <#session|message|#signatureK(#session|#message/sequence|#message/envelope)>
```

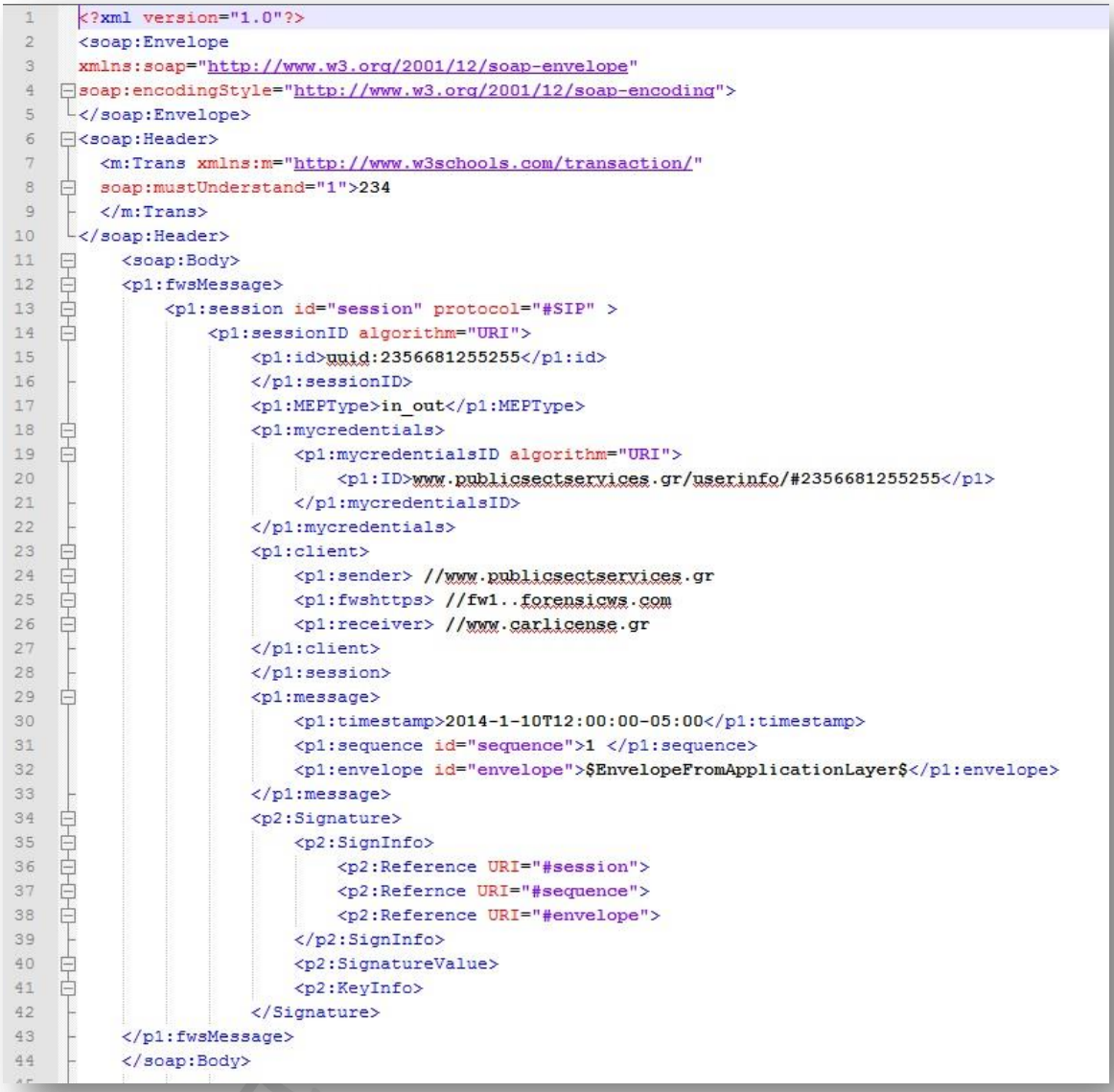
Όπου # γίνεται αναφορά σε σημεία της XML μορφής, η μπάρα | δηλώνει σύνδεση μεταξύ των εντολών των γραμμών για παράδειγμα <#message|#signatureK> , στο μήνυμα εμπεριέχεται και η υπογραφή του K αποστολέα.Το #session προσδιορίζει την επικοινωνία των Δικανικών Web υπηρεσιών. Το #message είναι το περιεχόμενο του ανώτερου επιπέδου σε μια επικοινωνία μεταξύ των Web υπηρεσιών. Και τα δύο τελικά σημεία (αποστολέα και παραλήπτη) υπογράφουν το #session.

Στο παράδειγμα που ακολουθεί το στοιχείο #session προσδιορίζει τις συνομιλίες των Δικανικών web υπηρεσιών, ένα μήνυμα αντιστοιχεί σε ένα στοιχείο που φέρει το πραγματικό μήνυμα του ανώτερου στρώματος μαζί με το αριθμό ακολουθίας του. Για παράδειγμα, ο αριθμός ακολουθίας 2 αντιστοιχεί σε ένα μήνυμα απάντησης εάν το μήνυμα χρησιμοποιεί πρότυπο ανταλλαγής μηνυμάτων two-way , όπως το πρότυπο MepType[20] και ένα πρωτόκολλο επικοινωνίας SIP[21]. Σε κάθε ακραίο σημείο, είτε ο αποστολέας είτε ο αποδέκτης υπογράφουν το session, μηνύματος/ακολουθίας και του μηνύματος/ envelop[22] μέρη του μηνύματος μέσα στο ds:Signature στοιχείο του μηνύματος. Ακολουθεί παράδειγμα ενός XML μηνύματος:

[20] MepType μοτίβο: Στις τηλεπικοινωνίες ένα πρότυπο ανταλλαγής μηνυμάτων MEP , περιγράφει την εξέλιξη των μηνυμάτων που απαιτούνται από ένα πρωτόκολλο επικοινωνιών για την αποκατάσταση ή να χρησιμοποιήσετε ένα κανάλι επικοινωνίας. Υπάρχουν δύο κύρια πρότυπα ανταλλαγής μηνυμάτων - ένα πρότυπο αίτησης-απάντησης(HTTP), και ένα μονόδρομο (UDP).

[21] Session Initiation protocol: Είναι πρωτόκολλο επικοινωνίας μέσω δικτύων υπολογιστών, που επιτρέπει την μεταφορά πολυμεσικών πληροφοριών είτε μέσω του διαδικτύου, είτε μέσω ενός τοπικού δικτύου. Για την εφαρμογή του απαιτείται η χρήση ενός υπολογιστή που να έχει τον ρόλο του εξυπηρετητή SIP (SIP server)

[22] XML Envelop: Το στοιχείο envelop χρησιμοποιείται για να συνδικάσει πολλαπλά έγγραφα XML σε ένα ενιαίο, έγκυρο μήνυμα.



```
<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">
</soap:Envelope>
<soap:Header>
  <m:Trans xmlns:m="http://www.w3schools.com/transaction/"
  soap:mustUnderstand="1">234
  </m:Trans>
</soap:Header>
    <soap:Body>
    <p1:fwsMessage>
        <p1:session id="session" protocol="#SIP" >
            <p1:sessionID algorithm="URI">
                <p1:id>uuid:2356681255255</p1:id>
                </p1:sessionID>
                <p1:MEPType>in_out</p1:MEPType>
                <p1:mycredentials>
                    <p1:mycredentialsID algorithm="URI">
                        <p1:ID>www.publicsectservices.gr/userinfo/#2356681255255</p1>
                    </p1:mycredentialsID>
                </p1:mycredentials>
                <p1:client>
                    <p1:sender> //www.publicsectservices.gr
                    <p1:fwshttps> //fw1..forensicws.com
                    <p1:receiver> //www.carlicense.gr
                </p1:client>
                </p1:session>
                <p1:message>
                    <p1:timestamp>2014-1-10T12:00:00-05:00</p1:timestamp>
                    <p1:sequence id="sequence">1 </p1:sequence>
                    <p1:envelope id="envelope">$EnvelopeFromApplicationLayer$</p1:envelope>
                </p1:message>
                <p2:Signature>
                    <p2:SignInfo>
                        <p2:Reference URI="#session">
                        <p2:Refernce URI="#sequence">
                        <p2:Reference URI="#envelope">
                    </p2:SignInfo>
                    <p2:SignatureValue>
                    <p2:KeyInfo>
                </Signature>
    </p1:fwsMessage>
    </soap:Body>
```

Οι Δικανικές υπηρεσίες Ιστού αποθηκεύουν τα μηνύματα με δύο μορφές, LogRecordIndex (LRI) και LogRecord (LR) χωρίς υπογραφές. Στις LRI εγγραφές καταγράφεται ένα απλό μήνυμα των Δικανικών υπηρεσιών ιστού ενώ το LogRecord αποθηκεύει ολόκληρα “sessions”, περιλαμβάνοντας όλα τα μηνύματα που παραλήφθηκαν ή δημιουργήθηκαν από μια web Δικανική υπηρεσία. Οι LRI εγγραφές αποθηκεύονται και στα δύο τερματικά σημεία (αποστολέα – παραλήπτη), ενώ τα Log Records (LR) μόνο στο σημείο του χειριστή (operator) των Δικανικών υπηρεσιών ιστού. Οι εγγραφές LRI χρησιμοποιούνται για δύο σκοπούς (i) για γρήγορες αναζητήσεις και (ii) για να παρακολουθείται η θέση ολόκληρου του LR.

- Όλες οι υπηρεσίες ιστού πρέπει να χρησιμοποιούν ένα πράκτορα (client agent) ο οποίος αναδρομολογεί όλα τα μηνύματα που διακινούνται μέσω των Web Δικανικών Εξυπηρετητών.

Οι Δικανικές υπηρεσίες προσθέτουν χρονοσήμανση (timestamp[23]) σε όλα τα μηνύματα. Τα LogRecords περιέχουν ένα κατάλογο των εγγραφών με την τελική χρονοσήμανση του κάθε μηνύματος, την κατάσταση και τη τιμή από την τελευταία επικοινωνία. Όλη η διακινούμενη πληροφορία αναδρομολογείται και καταγράφεται μέσω των Δικανικών Εξυπηρετητών χρησιμοποιώντας τις διαδικασίες μπροστά από κάθε endpoint των web υπηρεσιών.

Στην εικόνα που ακολουθεί παρουσιάζεται ένα XML μήνυμα, τα τμήματα με τα χρωματιστά πλαίσια αποτελούν τα κομμάτια αυτά του μηνύματος που καταγράφονται από τον διαμεσολαβητή. Οι Δικανικές Υπηρεσίες ιστού που αναλαμβάνουν να αποθηκεύσουν LRI εγγραφές θέτουν την τιμή σε ένα πεδίο «status» που κατέχουν, αναλόγως με την τιμή που έχει το message/sequence κομμάτι του Δικανικού μηνύματος. Για παράδειγμα και συμφώνα με την παρακάτω εικόνα, το μήνυμα με timestamp στις 9:56 και sequence 1 , κόκκινο πλαίσιο, θα καταγραφεί με «status» ίσο με 1 , το μήνυμα με sequence αριθμό 2 θα καταγραφεί με «status» ίσο με 2 και ούτω κάθε εξής.

Επίσης, οι Δικανικές υπηρεσίες ιστού καταγράφουν την τιμή timestamp από το κομμάτι message/timestamp του μηνύματος καθώς και το “recordinfo” με την αντίστοιχη τιμή που έχει το session κομμάτι του μηνύματος (sessionID).

```
//LR and LRI ex for 2 messages//
        <p1:session>
<p1:logRecord>
    <p1:recordIndex>
    <p1:timestamp>10:00</p1:timestamp>
    <p1:status>3</p1:status>
    <p1:recordInfo protocol="URI">
        <p1:sessionID algorithm="URI">
        <p1:MEPType>in_out</p1:MEPType>
        <p1:mycredentials/>
        <p1:clients>
            <p1:sender/>
            <p1:fwsttp/>
            <p1:receiver/>
        </p1:client>
    </p1:recordInfo>
    <p1:recordIndex>
    <p1:fwsMessage>
        <p1:session/>
        <p1:message/>
            <p1:timestamp>9:56</p1:timestamp>
            <p1:sequence>1</p1:sequence>
            <p1:envelope>msg...</p1:envelope>
        <p1:message>
        <ds:signature/>
    </p1:fwsMessage>
    <p1:fwsMessage>
        <p1:session/>
        <p1:message/>
            <p1:timestamp>9:58</p1:timestamp>
            <p1:sequence>2</p1:sequence>
            <p1:envelope>...</p1:envelope>
        <p1:message>
        <ds:signature/>
    </p1:fwsMessage>
    <p1:fws:Message>
        <p1:session/>
        <p1:message/>
            <p1:timestamp>10:00</p1:timestamp>
            <p1:sequence>3</p1:sequence>
            <p1:envelope>...</p1:envelope>
        <p1:message>
        <ds:signature/>
    </p1:fwsMessage>
</p1:logRecord>
```

Εικόνα 15. Δείγμα LRI και LR εγγραφών.

[23] Timestamp: Σαν χρονοσήμανση ορίζεται η ακριβής ώρα ενός γεγονότος (event), χρησιμοποιώντας κάποιους μηχανισμούς όπως το πρωτόκολλο NTP (Network Time Protocol). (http://whatis.techtarget.com/definition/timestamp).

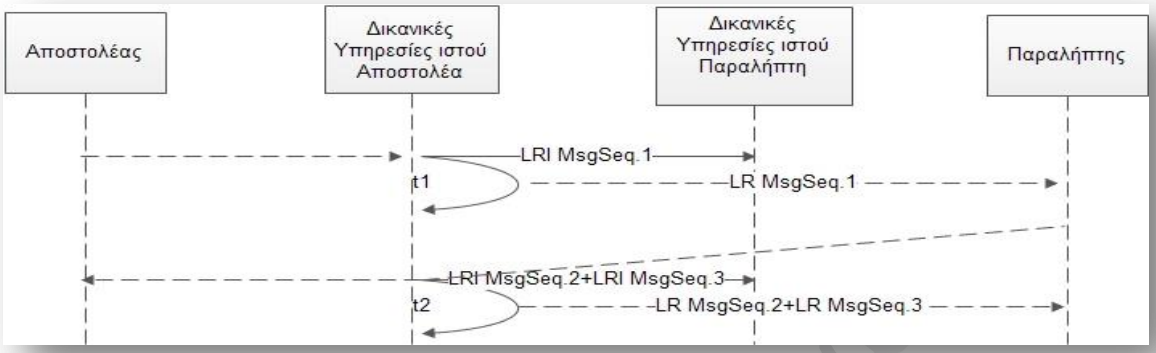
Η δρομολόγηση μέσω των Δικανικών εξυπηρετητών προϋποθέτει ότι όλες συναλλαγές θα είναι αξιόπιστες και θα δρομολογούνται. Όπως έχει αναφερθεί και ανωτέρω, οι εξυπηρετητές των Δικανικών υπηρεσιών ιστού, συλλέγουν ζεύγη αποδεικτικών στοιχείων που «κινούνται» μεταξύ του αποστολέα ,του παραλήπτη και του παραλήπτη των υπηρεσιών ιστού, κάνοντας χρήση του πρωτόκολλου SIP. Υπάρχουν τέσσερις οντότητες όπως αυτές έχουν περιγραφεί στην αρχή της ενότητας (σελ. 32) που συμμετέχουν στην διαδικασία , ο «Χειριστής» των Δικανικών υπηρεσιών αναλαμβάνει την εκτέλεση των παρακάτω βημάτων μεταξύ του αποστολέα και του παραλήπτη των μηνυμάτων:

- Οι Δικανικές υπηρεσίες ιστού λαμβάνουν MessageSeq.1. (<#session|#ds:signature(#session|1|#envelope)>).
- Επικυρώνει και αποθηκεύει το μήνυμα, δημιουργεί ένα LR και ένα LRI για το MessageSeq.1και ειδοποιεί τον χειριστή όλων των υπολοίπων web υπηρεσιών όπου δεν εμπλέκονται στους web Δικανικούς μηχανισμούς.
- Το MessageSeq.1 προωθείται στον αποδέκτη και γίνεται εκκίνηση του χρονομέτρου (timer).
- Εάν το μήνυμα απάντησης, MessageSeq.2 δεν φτάσει στις Δικανικές υπηρεσίες ιστού στο συγκριμένο χρονικό περιθώριο που ορίστηκε από το χρονόμετρο, τότε το MessageSeq.1 υπογράφεται από τους Δικανικές υπηρεσίες αποθηκεύεται, αποστέλλεται πίσω στον αποστολέα και τέλος δημιουργείται ένα LRI το οποίο αποστέλλεται στους non-operator χειριστές.

  Εάν το MessageSeq.2 (<#session|#ds:signature(#session|2|#envelope)>) παραληφτεί εντός των χρονικών ορίων που έχουν τεθεί και περάσει κάποια τεστ εγκυρότητας, προωθείται στον αποστολέα και αποθηκεύεται στους Δικανικούς εξυπηρετητές ενημερώνοντας ταυτόχρονα τις non-operator Δικανικές υπηρεσίες με το LRI που φέρει.

  Στην τελευταία περίπτωση αν MessageSeq.2 αποτύχει στα τεστ εγκυρότητας, υπογράφεται από τις Δικανικές υπηρεσίες ιστού , αποθηκεύεται και αποστέλλεται πίσω στον αποστολέα, καθώς επίσης ένα LRI δημιουργείται και αποστέλλεται στις non-operator Δικανικές υπηρεσίες.
- Τέλος, οι Δικανικές υπηρεσίες ιστού δημιουργούν, υπογράφουν και αποστέλλουν ένα MessageSeq.3 (<#session|#ds:signature(#session|3|#envelope)>), στον παραλήπτη. Επίσης αποθηκεύουν το μήνυμα μέσα σε ένα LR και αποστέλλουν ένα LRI στις non-operator Δικανικές υπηρεσίες.

Στο σχήμα που ακολουθεί απεικονίζεται γραφικά η διαδικασία αποθήκευσης μηνύματος μιας Δικανικής υπηρεσίας ιστού.



Εικόνα 16. Αποθήκευσης μηνύματος Δικανικής υπηρεσίας ιστού

3.1.3.3 Δημιουργία αποδεικτικών στοιχείων

Όπως έχει αναφερθεί ο κύριος σκοπός του πλαισίου των Δικανικών υπηρεσιών είναι η μετέπειτα διερεύνηση αποδεικτικών στοιχείων μεταξύ αλληλοσχετιζόμενων γεγονότων τα οποία αποθηκεύονται σε πολλαπλές Δικανικές υπηρεσίες ιστού. Τα στοιχεία συλλέγονται βάσει κάποιων συμπεριφορικών αλληλουχιών, συμπεριφορές που αποτελούνται από αλληλουχία γεγονότων, περιορισμών στις τιμές των δεδομένων και συγχρονισμού των δεδομένων. Η συμπεριφορική ακολουθία έχει δύο περιορισμούς:

- Χρονικούς περιορισμούς, οι οποίοι περιγράφουν την εκκίνηση και/ή τον τερματισμό ενός επιτυχούς ή ανεπιτυχούς υπολογισμού. Ένα τέτοιο παράδειγμα είναι ο μέγιστος χρόνος απόκρισης ενός χειριστή γεγονότων (event handler).
- Περιορισμοί χρονοσειρών. Περιγράφουν την χρονική διάρκεια μιας σειράς υπολογισμών που θα πρέπει να εκτελεστούν σε ένα συγκεκριμένο χρόνο. Για παράδειγμα όταν το system load ξεπερνάει το 75% του μέγιστου «φορτίου» , τότε θα πρέπει να μειωθεί στο 50% του μέγιστου «φορτίου» μέσα σε ένα λεπτό και θα πρέπει να παραμείνει μέχρι ή και λιγότερο από 60% του «φορτίου» για λιγότερο από δέκα λεπτά.

Τα αρχεία καταγραφής συμβάντων περιέχουν όλα τα αποδεικτικά στοιχεία τα οποία θα χρησιμοποιηθούν για την τεκμηρίωση των διαφόρων υποθέσεων, είναι τα παρακάτω:

- Αποδεικτικά στοιχεία προέλευσης (Evidence of Origin). Περιλαμβάνει πιστοποίηση της ώρας αποστολής και προέλευσης του μηνύματος.
- Αποδεικτικά στοιχεία παράδοσης (Evidence of Delivery). Περιλαμβάνει το μήνυμα αποδοχής από τον παραλήπτη για το οποίο προοριζόταν το μήνυμα .
- Αποδεικτικά στοιχεία αποτυχίας αποστολής (Evidence of Failure). Περιλαμβάνει την καταγραφή επιβεβαίωσής του μηνύματος που δεν παραδόθηκε έγκαιρα στον παραλήπτη ή δεν βρέθηκε ο συγκεκριμένος παραλήπτης.
- Αποδεικτικά στοιχεία διαθεσιμότητας (Evidence of Availability). Καταγράφει την διαθεσιμότητα των εξυπηρετητών (servers) σε ένα συγκεκριμένο χρονικό διάστημα.
- Αποδεικτικά στοιχεία παραβίασης της εγκυρότητας (Evidence of Agreement Violation). Περιλαμβάνει καταγραφή για τυχόν παραβίασης εγκυρότητας του Δικανικού εξυπηρετητή.

Στο παρακάτω πίνακα παρουσιάζονται, σε συνδυασμό με την Εικόνα 16 , ή εφαρμογή του πλαισίου των Δικανικών υπηρεσιών σε σχέση με τους τύπους των αποδεικτικών στοιχείων όπως αυτά έχουν περιγραφτεί στην προηγούμενη παράγραφο.

Τύπος Αποδεικτικών Στοιχείων	Υπογράφων της συναλλαγής	Πλαίσιο Δικανικής Υπηρεσίας
Evidence of Origin	Αποστολέας του μηνύματος	MessageSeq.1 & MessageSeq.3
Evidence of Delivery	Αποδέκτης του μηνύματος	MessageSeq.1 & MessageSeq.2
Evidence of Failure	Δικανικές Υπηρεσίες	MessageSeq.-1
Evidence of Availability	Δικανικές Υπηρεσίες	MessageSeq.0
Evidence of Agreement Violation	Δικανικές Υπηρεσίες	MessageSeq.-2

Πίνακας 1. Τύποι αποδεικτικών στοιχείων.

Όπως έχει προαναφερθεί , ο κύριος στόχος του πλαισίου των Δικανικών υπηρεσιών ιστού είναι η έρευνα που ακολουθεί μετά από ένα συμβάν επίθεσης η οποία αποτελείται από αλληλοεξαρτώμενα σενάρια και μπορεί να επιτευχθεί χρησιμοποιώντας τις ακόλουθες διαδικασίες:

1. Καθορισμός των ορίων μέσα στο οποίο συνέβη το συμβάν της επίθεσης, προσδιορίζοντας για το ποιες υπηρεσίες ιστού θα τεθούν υπό διερεύνηση (αποκαλούνται και «ύποπτες» υπηρεσίες ιστού) καθώς και η χρονική διάρκεια περίοδος του συμβάντος.
2. Καταγραφή της αλληλουχίας και της συμπεριφοράς των συσχετιζόμενων «ύποπτών» υπηρεσιών ιστού. Στην συγκεκριμένη διαδικασία συλλέγονται συμβάντα τα οποία προκαλούν την ανεπιτυχή εκτέλεση των υπηρεσιών ιστού.
3. Χρήση της registry των Δικανικών εξυπηρετητών ιστού έτσι ώστε να εντοπισθούν οι LR εγγραφές που μπορεί να εμπεριέχουν συναλλαγές από κακόβουλες υπηρεσίες ιστού.
4. Ανάκτηση από ζεύγη συναλλαγών που περιέχουν αποδεικτικά στοιχεία από μια συγκεκριμένη χρονική περίοδο.
5. Τέλος, γίνεται η αναδημιουργία των διάφορων συναλλαγών που συνέβησαν μεταξύ των υπηρεσιών ιστού έτσι ώστε να ανακατασκευαστεί η επίθεση.

Συνοψίζοντας, η μεθοδολογία των Υπηρεσιών Ιστού παρουσιάζει ένα πλαίσιο που δίνει την δυνατότητα να γίνεται καταγραφή των συναλλαγών μεταξύ των υπηρεσιών και παρακολούθηση τους σε πραγματικό χρόνο έτσι ώστε να αυτοματοποιηθεί η δημιουργία αποδεικτικών στοιχείων για σύνθετα σενάρια επιθέσεων.

3.2 Αξιολόγηση Μεθοδολογιών

Στην τρέχουσα ενότητα θα γίνει μια σύντομη αναδρομή αρχικά καθώς και η αξιολόγηση των τριών μεθοδολογιών (εν. 3.1.1-3.1.3). Θα επισημανθούν τα θετικά σημεία, οι παραλήψεις της κάθε μεθοδολογίας καθώς και οι μεταξύ τους διαφορές. Τέλος θα γίνει πρόταση μιας ιδανικής μεθοδολογίας η οποία αποτελεί σύνθεση των τριών περιγραφέντων μεθοδολογιών η οποία θα καλύπτει την προστασία ενός περιβάλλοντος υπηρεσιών ιστού σε τεχνικό επίπεδο καθώς και σε επίπεδο θεωρητικό κατά την συλλογή στοιχείων που θα περιέχουν αποδεικτικά στοιχεία τα οποία θα μπορούν να παρουσιαστούν σε μια Δικαστική αρχή.

Επιπροσθέτως, η μεθοδολογία που θα εξαχθεί, η οποία θα αποτελεί σύνθεση των προαναφερθέντων μεθοδολογιών, θα έχει προσανατολισμό στις υπηρεσίες ιστού (web services) και για το πώς θα μπορέσει να εφαρμοστεί ένα πλαίσιο μεθοδολογιών οι οποίες θα πλαισιώνονται από τα κατάλληλα εργαλεία με στόχο να εξασφαλίζουν τις ασφαλείς συναλλαγές μεταξύ των υπηρεσιών πελάτη – εξυπηρετητή, να τις καταγράφουν και να παρέχουν όλα τα δεδομένα αυτά που θα επιτρέπουν την ανακατασκευή ενός συμβάντος και την συλλογή όλων των πληροφοριών οι οποίες θα αποτελούν πειστήρια σε μια ενδεχόμενη επίθεση.

3.2.1 Αξιολόγηση «Μεθοδολογίας τριών βημάτων»

Σύμφωνα με την πρώτη μεθοδολογία, την «Μεθοδολογία των τριών βημάτων», οι διαδικασίες επικεντρώνονται σε τρία βασικά σημεία. Πριν από την εφαρμογή των βασικών βημάτων, θα πρέπει να προηγηθεί ακριβές και λειτουργικό αντίγραφο των εγκληματολογικών δεδομένων, δηλαδή ακριβής απεικόνιση του συστήματος μετά την εγκληματική ενέργεια. Αφού δημιουργηθεί ένα πιστό αντίγραφο των γνήσιων δεδομένων, ακολουθεί η διαδικασία της εξαγωγής των δεδομένων έτσι ώστε να αξιολογηθούν και να ταξινομηθούν στις κατάλληλες «λίστες αναζήτησης – αποτελεσμάτων».

Στο δεύτερο βήμα της μεθοδολογίας γίνεται η εξακρίβωση των δεδομένων, κάθε αντικείμενο της «Λίστας εξαγόμενων δεδομένων» του πρώτου βήματος. Κατά την διάρκεια της έρευνας αν κάποιο στοιχείο-αντικείμενο θεωρηθεί ότι δεν προσφέρει κάποια δεδομένα στην εγκληματολογική έρευνα καταχωρείται στη σχετική λίστα σαν επεξεργασμένο. Αν κάποιο αντικείμενο θεωρηθεί εκτός του ερευνητικού πεδίου της έρευνας, η εγκληματολογική εξέταση σταματάει και το αντικείμενο τοποθετείται στην σχετική λίστα. Τα αντικείμενα που αποτελούν αποδεικτικά στοιχεία τα οποία καταδεικνύουν μια ψηφιακή επίθεση τοποθετούνται σε μια τρίτη λίστα - «Λίστα σχετικών δεδομένων». Για κάθε νέο ενοχοποιητικό στοιχείο που προκύπτει, ο ειδικός ερευνητής τοποθετεί το αντικείμενο σε μια τέταρτη λίστα αυτή της «Νέας πηγής της λίστας δεδομένων».

Στο τελευταίο στάδιο της μεθοδολογίας, γίνεται η ανάλυση των δεδομένων που συλλέχθηκαν στις προηγούμενες διαδικασίες. Στο βήμα της ανάλυσης γίνεται ανακατασκευή της επίθεσης έτσι ώστε να εξαχθούν τα απαραίτητα δεδομένα που θα οδηγήσουν σε μια Εγκληματολογική Αναφορά. Τα δεδομένα που προκύπτουν προστίθενται στη «Λίστα Ανάλυσης Αποτελεσμάτων» και υποδεικνύουν τον τρόπο, τον υπεύθυνο της επίθεσης καθώς και τη χρονική σειρά των συμβάντων της επίθεσης.

Η μεθοδολογία των τριών βημάτων θα μπορούσε να χαρακτηριστεί σαν μια Δραστική μεθοδολογία (Reactive), δηλαδή έχει εφαρμογή μόνο μετά την ύπαρξη ενός συμβάντος επίθεσης. Στα θετικά σημεία της μεθοδολογίας των τριών βημάτων συγκαταλέγεται το γεγονός ότι αποτελεί μια δομημένη διαδικασία με σαφή βήματα. Στα πλεονεκτήματα συμπεριλαμβάνεται η δυνατότητα επανεξέτασης και ταξινόμησης των διαφόρων αντικειμένων – πειστηρίων. Σε κάθε περίπτωση ο εγκληματολογικός ερευνητής έχει την δυνατότητα να «τρέξει» τη διαδικασία πολλές φορές έτσι ώστε να εξάγει ασφαλή συμπεράσματα και να αποκτήσει επαρκή αποδεικτικά στοιχεία για μια ποινική δίωξη. Τα βασικά εργαλεία στα οποία στηρίζεται η μέθοδος των τριών βημάτων είναι η ύπαρξη των Λιστών ταξινόμησης των αντικειμένων της εξέτασης, η απλότητα στην εφαρμογή της σε οποιοδήποτε περιβάλλον, ευκολία στην επανεξέταση νέων στοιχείων που θα προκύψουν από μια έρευνα.

Η «Μεθοδολογία των τριών βημάτων» παρουσιάζει αρκετά μειονεκτήματα καθώς, όπως έχει ήδη αναφερθεί είναι μία (Reactive) Δραστική μεθοδολογία. Ο ειδικός ερευνητής δημιουργεί αντίγραφο των εγκληματολογικών δεδομένων μετά το συμβάν της επίθεσης, έτσι ώστε να ανακατασκευάσει στη συνέχεια την επίθεση αυτή. Στην περίπτωση αυτή εάν δεν υπάρχουν τα κατάλληλα αντίμετρα

από τη μεριά του διαχειριστή των συστημάτων ενός οργανισμού θα μπορούσε κάλλιστα κάποιος εγκληματίας με ειδικές γνώσεις να καλύψει τα ίχνη της επίθεσης. Ακόμα, αμφισβητείται η εγκυρότητα των γνήσιων δεδομένων καθώς ο εγκληματολόγος της Δικανικής Πληροφορικής δεν είναι σε θέση να γνωρίζει εάν ο διαχειριστής των συστημάτων και του τεχνολογικού περιβάλλοντος του οργανισμού που έχει υποστεί μια ηλεκτρονική επίθεση, έχει κάνει όλες τις απαραίτητες ενέργειες για την ορθή και ασφαλή λειτουργία των συστημάτων (ενημερώσεις λογισμικού, firewall, αρχεία log). Συμπεραίνεται ότι υπάρχει πάντα ο κίνδυνος στο εικονικό αρχείο που θα δημιουργηθεί από τον ειδικό ερευνητή και θα αποτελεί πιστό αντίγραφο των γνήσιων δεδομένων του πληροφοριακού συστήματος, τα στοιχεία αυτά να έχουν αλλοιωθεί εσκεμμένα ή από αμέλεια του διαχειριστή, με αποτέλεσμα να εξαχθούν λανθασμένα και ελλιπή αποτελέσματα. Στην λίστα των μειονεκτημάτων προστίθεται και το γεγονός ότι η «Μεθοδολογία των τριών βημάτων» είναι μια γενική μεθοδολογία, που μεν την καθιστά εύκολα προσαρμόσιμη σε διάφορα υπολογιστικά περιβάλλοντα αλλά στο πεδίο των υπηρεσιών ιστού (web services) θα καθιστούσε δύσκολη την ανάκτηση των δεδομένων της επίθεσης καθώς οι υπηρεσίες ιστού προϋποθέτουν τα πληροφοριακά συστήματα να παρέχουν όλα αυτά τα εργαλεία που θα επιτρέπουν τη συλλογή «ζωντανών» αποδεικτικών στοιχείων σε πραγματικό χρόνο και να καταγράφουν τις συναλλαγές μεταξύ των διάφορων υπηρεσιών.

3.2.2 Αξιολόγηση «Μεθοδολογίας Πολλαπλών Συνιστωσών»

Στη μεθοδολογία Πολλαπλών Συνιστωσών ή διαφορετικά μεθοδολογία Gobler – Louwrens – Solms, συναντώνται τρείς συνιστώσες που την απαρτίζουν, αυτές της προληπτικής Ψηφιακής Εγκληματολογίας, της Δραστικής εγκληματολογίας και τέλος της ενεργής ψηφιακής εγκληματολογίας.

Κατά τη διαδικασία της Προληπτικής ψηφιακής Εγκληματολογίας, καθορίζονται όλες αυτές οι διαδικασίες οι οποίες θα βοηθήσουν στη συλλογή, τη φύλαξη και τη διαχείριση όλων των ψηφιακών αποδείξεων που θα οδηγήσουν σε μια αποτελεσματική έρευνα ενός συμβάντος ηλεκτρονικής επίθεσης. Γίνεται η κατάλληλη μελέτη και προετοιμασία στις υποδομές του πληροφοριακού συστήματος καθώς επίσης και στην οργάνωση σχεδίου αντιμετώπισης κινδύνων. Επιπροσθέτως, αναπτύσσεται ένα σχέδιο διαχείρισης που θα αποβλέπει στη συλλογή, διαχείριση και ανάκτηση όλων των ψηφιακών πειστηρίων μετά από ένα συμβάν επίθεσης. Ένας οργανισμός θα πρέπει να προσαρμόσει όλα αυτά τα εργαλεία της ψηφιακής τεχνολογίας (Digital Forensics) που θα έχουν την ικανότητα να καταγράφουν μια εγκληματική πράξη στοχεύοντας στην ασφάλεια του οργανισμού. Επίσης, γίνεται πρόβλεψη για το κόστος μιας μελλοντικής έρευνας, όλες οι μέθοδοι που θα εφαρμοστούν προαποφασίζονται και επικυρώνονται εγγράφως και τέλος ο οργανισμός είναι υπεύθυνος να ορίσει ένα άτομο το οποίο θα είναι υπεύθυνο και θα είναι εξουσιοδοτημένο να διαχειρίζεται και να επιβλέπει όλα τα εργαλεία της που θα βοηθήσουν μια επικείμενη Δικανική έρευνα.

Η δεύτερη συνιστώσα είναι αυτή της Δραστικής Ψηφιακής εγκληματολογίας (Reactive Digital Forensics). Η μέθοδος χωρίζεται σε έξι φάσεις κατά τις οποίες εφαρμόζονται τεχνικές οι οποίες εξασφαλίζουν την απομόνωση του φυσικού περιβάλλοντος, τη συλλογή και διαφύλαξη των αποδεικτικών στοιχείων καθώς επίσης και την ταυτοποίηση τους. Τα αποδεικτικά στοιχεία μεταφέρονται και αποθηκεύονται έτσι ώστε να μην υποστούν κάποια αλλοίωση. Στα βήματα που ακολουθούν γίνεται προσπάθεια ανακατασκευής της επίθεσης, διατυπώνοντας εγγράφως ένα υποθετικό σενάριο το οποίο εφαρμόζεται πειραματικά. Για να εξαχθούν όσα περισσότερα ακριβή στοιχεία οι φάσεις (δύο και τρία όπως περιγράφονται αναλυτικά στην ενότητα 3.1.2) μπορούν να επαναληφθούν αρκετές φορές. Στα τελευταία στάδια της μεθόδου παρουσιάζονται τα ευρήματα των προηγούμενων φάσεων και γίνεται η ανακοίνωση των αποτελεσμάτων έτσι ώστε να κλείσει η

υπόθεση της ηλεκτρονικής επίθεσης και να διωχθούν νομικά οι δράστες. Οι φάσεις της Δραστικής Ψηφιακής εγκληματολογίας μπορούν απεικονιστούν με ένα μοντέλο καταρράκτη.

Η τελευταία συνιστώσα της μεθοδολογίας είναι αυτή της Ενεργής Ψηφιακής Εγκληματολογίας. Στη κλασσική μέθοδο της Δραστικής Ψηφιακής εγκληματολογίας είναι σχεδόν αδύνατο να ανιχνεύσουν τυχόν αλλαγές που θα γίνουν στα «ζωντανά» πληροφοριακά συστήματα κατά την διάρκεια της έρευνας. Την αδυναμία αυτή έρχεται να καλύψει η Ενεργή Ψηφιακή Εγκληματολογία κάνοντας χρήση εργαλείων που εξασφαλίζουν ότι δεν θα υπάρξουν αλλαγές στα αποδεικτικά στοιχεία που συλλέγονται. Σύμφωνα με τη μεθοδολογία είναι απαραίτητη η χρήση εργαλείων ανίχνευσης εισβολών (IDS) και Incident Response πρωτοκόλλων (IR), τα οποία αποτελούν σχέδια για το πώς θα αντιμετωπιστούν οι συνέπειες παραβίασης των πληροφοριακών συστημάτων ενός οργανισμού. Σύμφωνα με την μεθοδολογία προτείνεται η χρήση ενός εξυπηρετητή (server) που θα έχει γίνει εγκατάσταση μιας ειδικής κάρτας PCI η οποία θα αναλαμβάνει την επίβλεψη του πληροφοριακού συστήματος και των «ζωντανών» δεδομένων του δικτυακού περιβάλλοντος. Η μέθοδος της Ενεργής Ψηφιακής Εγκληματολογίας περιλαμβάνει τέσσερις φάσεις. Στην πρώτη φάση εκτελούνται τα βήματα της δραστικής ψηφιακής μεθόδου με τη μόνη διαφορά ότι θα πρέπει να διαχωριστούν για τα ποια αποδεικτικά στοιχεία αποτελούν «ζωντανές» ψηφιακές ενδείξεις. Εφόσον εντοπιστούν τα «ζωντανά» πειστήρια, συλλέγονται και αποθηκεύονται όπως συμβαίνει και στην Τρίτη φάση της δραστικής ψηφιακής εγκληματολογίας. Στη συνέχεια γίνεται ανάλυση των πειστηρίων και η ανακατασκευή του συμβάντος της επίθεσης. Αν δεν επαρκούν τα στοιχεία για διαλεύκανση του ψηφιακού εγκλήματος τότε η μέθοδος μπορεί να επαναληφθεί αρκετές φορές έως ότου τερματιστεί η διαδικασία. Κατά την τελική φάση και εφόσον έχουν συλλεχθεί αρκετά αποδεικτικά στοιχεία, προετοιμάζονται τα τεκμηριωμένα έγγραφα της υπόθεσης έτσι ώστε να συνεχίσει η διαδικασία της δραστικής ψηφιακής εγκληματολογίας.

Εντοπίζοντας τα θετικά σημεία της μεθόδου, αξίζει να αναφερθεί ότι η μεθοδολογία Πολλαπλών Συνιστωσών, αξίζει να σημειωθεί ότι καλύπτει όλα τα στάδια της Δικανικής έρευνας. Περιλαμβάνει προληπτικές μεθόδους, ακολουθεί αυστηρό πλαίσιο διαδικασιών για τα «ζωντανά» αλλά και για τα κοινά αποδεικτικά στοιχεία. Αναθέτει συγκεκριμένους ρόλους και ευθύνες όταν ενεργοποιηθούν οι μηχανισμοί της Δικανικής έρευνας. Προτείνει μετά από την σχετική μελέτη την εγκατάσταση όλων των εργαλείων που θα αποτρέψουν μια ηλεκτρονική επίθεση και θα συλλέξουν όλα τα απαραίτητα δεδομένα. Εμπεριέχει όλες τις δικλίδες ασφαλείας για τη συλλογή, φύλαξη και ανάλυση των πρότυπων πειστηρίων ενός περιβάλλοντος. Τέλος, δημιουργείται προμελετημένο πλαίσιο διαδικασιών για κάθε φάση της ένταξης ενός τεχνολογικού περιβάλλοντος σε Δικανικές μεθόδους, που θα είναι σε θέση να αντιμετωπίσουν αποτελεσματικά μια επίθεση ηλεκτρονικών εγκληματιών και να συλλέξουν τα απαραίτητα πειστήρια που θα παρουσιαστούν στις Δικαστικές αρχές.

Η μεθοδολογία των Πολλαπλών Συνιστωσών παρουσιάζει μερικά σημαντικά μειονεκτήματα. Αρχικά, αποτελεί μια αρκετά δαπανηρή λύση καθώς η εφαρμογή της προϋποθέτει την εγκατάσταση ειδικού εξοπλισμού, εξυπηρετητές με εγκατεστημένη κάρτα PCI οι οποίοι θα αναλαμβάνουν την εποπτεία του τεχνολογικού περιβάλλοντος του οργανισμού, καθώς επίσης και την πρόσληψη ειδικών επιστημών της Δικανικής πληροφορικής, οι οποίοι θα σχεδιάσουν σύμφωνα με τις απαιτήσεις ενός οργανισμού το πλαίσιο λειτουργίας του, θα κάνουν τον προληπτικό σχεδιασμό, θα εγκαταστήσουν τα εποπτικά εργαλεία και θα αναλάβουν την εκπαίδευση του προσωπικού καθώς και την ανάθεση των αρμοδιοτήτων. Η μεθοδολογία εμπεριέχει αρκετή πολυπλοκότητα με τον κίνδυνο μια έρευνα να αποδειχθεί χρονοβόρα. Κάθε φάση του θα πρέπει να σχεδιαστεί με μεγάλη λεπτομέρεια έτσι ώστε να αποδειχθεί αποτελεσματική. Τέλος, η μεθοδολογία των Πολλαπλών Συνιστωσών περιλαμβάνει μηχανισμούς

για την αντιμετώπιση και συλλογή «ζωντανών» αποδεικτών στοιχείων, αλλά εστιάζει περισσότερο σε τεχνικές που αφορούν την δικτυακή κίνηση δεδομένων ενός οργανισμού και όχι στις συναλλαγές μεταξύ των υπηρεσιών ιστού. Συμπεραίνουμε λοιπόν ότι παρουσιάζεται σημαντική ευπάθεια στην αντιμετώπιση επιθέσεων και την συλλογή πληροφοριών που αφορούν τις διαδικτυακές υπηρεσίες ενός οργανισμού τα αρχεία καταγραφής ή τα εργαλεία ειδοποιήσεων (incident response), έχουν μικρή εγκληματολογική αξία.

3.2.3 Αξιολόγηση «Μεθοδολογίας στα Web Services»

Η «Μεθοδολογία των Web Services» έχει σαν κύριο στόχο την διαφύλαξη της αξιοπιστίας τις συνδυαστικής λειτουργίας μεταξύ δύο ή περισσοτέρων υπηρεσιών ιστού. Η εφαρμογή της μεθοδολογίας προϋποθέτει την ύπαρξη μιας ανεξάρτητης έμπιστης αρχής (TTP – Trusted Third Party) η οποία θα είναι υπεύθυνη για την αυθεντικοποίηση των συναλλαγών μεταξύ των υπηρεσιών ιστού, την αξιόπιστη ανταλλαγή μηνυμάτων και την διατήρηση της αξιοπιστίας των καναλιών επικοινωνίας. Οι αξιόπιστες τρίτες αρχές είναι συνήθως εξυπηρετητές που αναλαμβάνουν την εποπτεία της ανταλλαγής μηνυμάτων μεταξύ των υπηρεσιών ιστού, διατηρώντας αρχεία καταγραφής (log records) στα οποία διατηρούνται πληροφορίες χρονοσήμανσης όπως χρόνος αίτησης μιας υπηρεσίας, χρόνος απόκρισης και λήξης της υπηρεσίας ενός αιτήματος και τέλος χρόνος διαθεσιμότητας ενός εξυπηρετητή που διατηρεί μια υπηρεσία ιστού. Τα στοιχεία που συλλέγονται στον αξιόπιστο «τρίτο» εξυπηρετητή, είναι απαραίτητα για την συλλογή των απαραίτητων πειστηρίων σε μια επικείμενη κακόβουλη ηλεκτρονική επίθεση καθώς και την ανακατασκευή του συμβάντος της επίθεσης. Για την τεκμηρίωση μιας Δικανικής έρευνας χρησιμοποιούνται οι εξής κατηγορίες αποδεικτικά στοιχεία προέλευσης, επιτυχούς ή μη επιτυχούς παράδοσης των μηνυμάτων, αποδεικτικά στοιχεία διαθεσιμότητας και παραβίασης της εγκυρότητας ενός Δικανικού εξυπηρετητή. Η καταγραφή των συναλλαγών μεταξύ των υπηρεσιών ιστού πραγματοποιείται σε πραγματικό χρόνο έτσι ώστε να αυτοματοποιηθεί η δημιουργία αποδεικτικών στοιχείων. Στην περίπτωση που εντοπιστεί μια κακόβουλη επίθεση στα ηλεκτρονικά συστήματα ενός οργανισμού και συγκεκριμένα στις υπάρχουσες υπηρεσίες ιστού, οι ειδικοί εγκληματολόγοι της Δικανικής Πληροφορικής, κάνουν χρήση των δεδομένων που έχουν καταγραφεί στους Δικανικούς εξυπηρετητές και ανακατασκευάζουν το σενάριο της επίθεσης βάση των χρονοσφραγίδων (timestamps) και της αλληλουχίας των συναλλαγών μεταξύ των εμπλεκόμενων υπηρεσιών πριν την έναρξη του συμβάντος της επίθεσης.

Το βασικό πλεονέκτημα της εν λόγω μεθοδολογίας είναι ότι εστιάζει στην αντιμετώπιση συμβάντων μεταξύ δύο ή περισσοτέρων υπηρεσιών ιστού ενός οργανισμού. Οι παραδοσιακές Δικανικές μέθοδοι και όπως έχει περιγραφτεί στις προηγούμενες ενότητες, υστερούν στην αντιμετώπιση «ζωντανών» επιθέσεων που αφορούν τις υπηρεσίες ιστού. Η μεθοδολογία καλύπτει και καταγράφει κάθε κομμάτι ανταλλαγής δεδομένων μεταξύ των υπηρεσιών που είναι απαραίτητο για την ανακατασκευή της επίθεσης και την διασφάλιση της ακεραιότητας του καναλιού επικοινωνίας. Η μεθοδολογία των υπηρεσιών ιστού παρουσιάζει ένα πλαίσιο απλοϊκών τεχνικών και εργαλείων της μπορούν εύκολα να εφαρμοστούν σε κάθε τεχνολογικό περιβάλλον όση πολυπλοκότητα και αν παρουσιάζει αυτό, αυτοματοποιώντας όλες τις λειτουργίες που θα ενισχύσουνε μια Δικανική έρευνα.

Τα μειονεκτήματα που παρουσιάζει η «Μεθοδολογία των Web Services» εστιάζονται στο ότι δεν υπάρχει συγκεκριμένο πλαίσιο φάσεων και βημάτων που θα πρέπει να ακολουθηθεί σε ένα συμβάν επίθεσης. Η εφαρμογή των εργαλείων καθώς και εποπτεία της καλής τους λειτουργίας απατούν ειδικές γνώσεις άρα το προσωπικό που διαχειρίζεται τα Δικανικά εργαλεία θα πρέπει να είναι κατάλληλα εκπαιδευμένο. Η μέθοδος στηρίζεται αποκλειστικά στην καλή εφαρμογή των

εργαλείων των Δικανικών εξυπηρετητών και δεν συμπεριλαμβάνει ελέγχους για το αν τα δεδομένα που συλλέχθηκαν μετά από κάποια ηλεκτρονική επίθεση είναι αρκετά για να συνταχθεί μια εγκληματολογική έκθεση. Δεν έχουν προβλεφθεί μηχανισμοί επανάληψης της διαδικασίας και τέλος δεν καθορίζονται οι ρόλοι κάθε εμπλεκόμενης μεριάς (διαχειριστών των συστημάτων, Δικανικών εγκληματολόγων) και για το πώς θα πρέπει να λειτουργήσουν σε ένα συμβάν ηλεκτρονικής επίθεσης.

3.2.4 Σύγκριση μεθοδολογιών - Βέλτιστη μεθοδολογία.

Τα ηλεκτρονικά εγκλήματα έχουν αυξηθεί σε συχνότητα και ο βαθμός της πολυπλοκότητας για την εξιχνίαση τέτοιου είδους εγκλημάτων έχει εξελίχθη. Οι ηλεκτρονικοί εγκληματίες χρησιμοποιούν τεχνικές αντί-εγκληματολογίας (anti-forensics παράγραφος 2.1.5), επιτυγχάνοντας να καλύψουν τα ίχνη μιας επίθεσης αποτελεσματικά με μεθόδους απόκρυψης των δεδομένων ή αλλοίωσης των δεδομένων. Τέτοιου είδους τεχνικές (14) είναι ικανές να αποτρέψουν την συλλογή των αποδεικτικών στοιχείων, να αυξήσουν το χρόνο της εγκληματολογικής έρευνας, να παρέχουν ψευδή πειστήρια που μπορούν να θέσουν σε κίνδυνο μια Δικανική έρευνα και τέλος να αποτρέψουν την ανίχνευση του ψηφιακού εγκλήματος.

Για να αναπτυχθεί ένας λειτουργικός ορισμός για τις Δικανικές διαδικασίες και τα σχετικά της στάδια, θα πρέπει να πραγματοποιηθεί μια συστηματική διαδικασία (SLR- Systematic Literature Review) η οποία θα επανεξετάζει, θα αναλύει και θα συνθέτει τα αποτελέσματα μιας έρευνας δημοσιοποιώντας τα σε έγγραφη μορφή σύμφωνα με τις διαδικασίες που ορίζει η Δικανική ψηφιακή έρευνα.

Είναι πολύ σημαντικό η διαδικασία αυτή (SLR) να καλύπτει όλα τα στάδια μιας έρευνας και συγκεκριμένα να έχει προνοήσει με τις κατάλληλες διαδικασίες και τα κατάλληλα εργαλεία την εποπτεία των συστημάτων ενός οργανισμού. Θα πρέπει να σχεδιάσει όλα τα προληπτικά μέτρα και τεχνολογικά εργαλεία (Proactive μεθοδολογίες), θα πρέπει να λάβει υπόψη την καταγραφή αξιόπιστων πληροφοριών σε πραγματικό χρόνο κατά την διάρκεια ενός συμβάντος. Θα πρέπει να εισάγει αυτοματισμούς χωρίς την παρέμβαση των χρηστών σε όλες τις φάσεις της ψηφιακής Δικανικής έρευνας. Απαραίτητη είναι η ανάγκη να υπάρχουν μηχανισμοί οι οποίοι θα διαχωρίζουν τα «ζωντανά» αποδεικτικά δεδομένα από αυτά της Δραστικής ψηφιακής μεθοδολογίας. Ιδιαίτερη βαρύτητα θα πρέπει να δοθεί στις υπηρεσίες ιστού οι οποίες διαφέρουν στον τρόπο αντιμετώπισης των απλών Δικανικών μεθόδων. Μια ολοκληρωμένη μεθοδολογία θα πρέπει λοιπόν να περιλαμβάνει σαφή βήματα και προκαθορισμένους ρόλους για κάθε επίπεδο και είδος της έρευνας (εγκλήματα πραγματικού χρόνου ή ψηφιακά εγκλήματα που αφορούν Δραστικές μεθόδους) αφού έχει προηγηθεί μελέτη αρχικά του τεχνολογικού περιβάλλοντος και των απαιτήσεων ενός οργανισμού ο οποίος παρουσιάζει την ανάγκη εφαρμογής Δικανικών εργαλείων. Τέλος, η συστηματική διαδικασία θα πρέπει να εξοικονομεί χρόνο και χρήματα σε ένα οργανισμό μειώνοντας τους διαθέσιμους πόρους που χρειάζονται για μια εγκληματολογική έρευνα.

Στις προηγούμενες ενότητες έγινε εκτενής αναφορά στα πλεονεκτήματα και τα μειονεκτήματα της κάθε μεθοδολογίας. Η μεθοδολογία των «τριών βημάτων» αποτελεί μια ολοκληρωμένη μέθοδο με σαφή βήματα η οποία είναι εύκολα εφαρμόσιμη σε διάφορα τεχνολογικά περιβάλλοντα, όμως βρίσκει εφαρμογή μόνο σε περιπτώσεις Δραστικής Δικανικής και δεν καλύπτει προληπτικές διαδικασίες ή συμβάντα πραγματικού χρόνου. Στα θετικά της μεθόδου συγκαταλέγεται η ύπαρξη Λιστών ταξινόμησης δεδομένων σχετικών με την υπόθεση της ψηφιακής επίθεσης κάτι που δεν υλοποιείται στις μεθοδολογίες «των Web Services» και των «Πολλαπλών Συνιστωσών». Η «Μεθοδολογία των Πολλαπλών Συνιστωσών» παρουσιάζεται σαν μια ολοκληρωμένη

μεθοδολογία κάνοντας χρήση προληπτικών εργαλείων, λαμβάνει υπόψη τη συλλογή και ανάλυση «ζωντανών» αποδείξεων και τέλος παρέχει ολοκληρωμένο πλαίσιο διαδικασιών για τις παραδοσιακές μεθόδους της Δικανικής πληροφορικής. Καθορίζει αναλυτικά τα βήματα που πρέπει να γίνουν πριν και μετά από ένα συμβάν ψηφιακής επίθεσης, καθώς επίσης αναλαμβάνει να θέσει τους ρόλους και τις αρμοδιότητες σε κάθε εμπλεκόμενο μέρος. Η μεθοδολογία των «Πολλαπλών Συνιστωσών», αποτελεί μια χρονοβόρα και δαπανηρή μέθοδο παρ' όλη την πληρότητα της σε όλα τα στάδια εφαρμογής της σε μια Δικανική έρευνα, αλλά επίσης παρουσιάζει έλλειψη στην αντιμετώπιση συμβάντων επιθέσεων που αφορούν υπηρεσίες ιστού. Το κενό στην Δικανική αντιμετώπιση υπηρεσιών ιστού έρχεται να καλύψει η «Μεθοδολογία των Web Services». Η προαναφερθείσα μεθοδολογία περιλαμβάνει όλα τα απαραίτητα εργαλεία και αυτοματισμούς που βοηθούν σε ένα συμβάν ψηφιακής επίθεσης και συγκεκριμένα σε γεγονότα που σχετίζονται με επίθεση πάνω σε υπηρεσίες ιστού ενός οργανισμού. Η «Μεθοδολογία των Web Services» εστιάζει μόνο στις τεχνολογίες ιστού και δεν παρέχει ένα ολοκληρωμένο πλαίσιο διαδικασιών το οποίο θα διασφαλίζει πλήρως ένα τεχνολογικό περιβάλλον, κάτι που μπορεί να επηρεάσει σε πολλά σημεία την εξαγωγή σωστών συμπερασμάτων και να δυσκολέψει την ανακατασκευή ενός σεναρίου επίθεσης στα web services μιας εταιρείας. Για παράδειγμα, αν μια υπηρεσία ιστού δεχθεί κάποιου είδους κακόβουλη επίθεση, σημαντικό ρόλο σε δικτυακό επίπεδο παίζει η ύπαρξη συστημάτων ανίχνευσης εισβολέων (IDS) και συστημάτων ανταπόκρισης συμβάντων (IR) που θα έχουν καταγράψει σημαντικές πληροφορίες για την διαλεύκανση της επίθεσης. Τέλος, η μέθοδος «Web Services» δεν παρουσιάζει συγκεκριμένα βήματα από τα αρχικά στάδια μιας εγκληματολογικής έρευνας έως ότου αυτή οδηγηθεί στις Δικαστικές Αρχές όπως αυτό συμβαίνει στις μεθοδολογίες των «Τριών Βημάτων» και των «Πολλαπλών Συνιστωσών», αλλά στηρίζεται μόνο στα τεχνολογικά της εργαλεία και τους αυτοματισμούς της.

Στο πίνακα που ακολουθεί παρουσιάζεται μια συνοπτική σύγκριση μεταξύ των μεθοδολογιών που έχουν περιγραφεί σε σχέση με το είδος της Δικανικής έρευνας που απαιτείται ανά περίπτωση.

Ψηφιακή Δικανική μεθοδολογία	**Προληπτική έρευνα**			**Ενεργή Ψηφιακή έρευνα**					**Δραστική έρευνα**					**Web Services**			**Αριθμός φάσεων**
	Συλλογή δεδομένων	Μηχανισμοί ενεργοποίησης συμβάντων	Προληπτική αντιμετώπιση συμβάντων	Ταυτοποίηση	Διαφύλαξη πειστηρίων	Συλλογή	Ανάλυση	Αναφορά	Ταυτοποίηση	Διαφύλαξη πειστηρίων	Συλλογή	Ανάλυση	Αναφορά	Συλλογή δεδομένων	ενεργοποίησης συμβάντων	Συλλογή\ Ανάλυση	--
«Μεθοδολογίας τριών βημάτων»	--	--	--	--	--	--	--	--	✓	✓	✓	✓	✓	--	--	--	3 φάσεις
«Μεθοδολογία Πολλαπλών Συνιστωσών»	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	--	--	--	3 κυρίως φάσεις συμπεριλα-μβανομένων υπο-φάσεων
«Μεθοδολογία Web Services»	✓	✓	✓	--	--	--	--	--	--	--	--	--	--	✓	✓	✓	2 φάσεις

Συμπερασματικά και βάση των μεθοδολογιών που παρουσιάστηκαν αναλυτικά, θέλοντας να κατασκευάσουμε μια ιδανική μεθοδολογία θα περιείχε τις εξής διαδικασίες εστιάζοντας στις Δικανική έρευνα των υπηρεσιών ιστού:

Φάση 1

Η πρώτη φάση αφορά τα προληπτικά (Proactive) μέτρα που θα πρέπει να ληφθούν έτσι ώστε να διασφαλισθεί η σωστή εποπτεία των ψηφιακών συστημάτων του οργανισμού και την ανάπτυξη μηχανισμών ειδοποίησης και αποτροπής ψηφιακών επιθέσεων.

Πρώτο βήμα: Αρχικά θα πρέπει να μελετηθεί το τεχνολογικό περιβάλλον του οργανισμού στο οποίο θα εφαρμοστούν οι τεχνικές της Δικανικής πληροφορικής καθώς επίσης και τα Δικανικά εργαλεία που θα πρέπει να εγκατασταθούν. Σε συνεργασία με τους ειδικούς και σύμφωνα με τις απαιτήσεις μιας Δικανικής.

Δεύτερο βήμα: Στο δεύτερο βήμα καθορίζονται οι ρόλοι του κάθε εμπλεκόμενου μέρους, αναλυτικότερα οι διαχειριστές των συστημάτων είναι υπεύθυνοι να συντηρούν και να αναβαθμίζουν τακτικά τον εξοπλισμό τους άλλα και το λογισμικό των συστημάτων. Η ομάδα ανάπτυξης λογισμικού της εταιρείας είναι υπεύθυνη στο να ελέγχει ή να διορθώνει τυχόν κενά στις διάφορες υπηρεσίες ιστού που μπορεί να υπάρχουν. Ο υπεύθυνος του τμήματος πληροφορικής του οργανισμού σε περίπτωση ανάγκης έρχεται σε επαφή με τους ειδικούς εγκληματολόγους της Δικανικής Πληροφορικής, έτσι ώστε να απομονωθεί το περιβάλλον και τα συστήματα που δέχθηκαν την κακόβουλη επίθεση και να ξεκινήσει η διαδικασία της έρευνας.

Τρίτο βήμα: Μετά από τις υποδείξεις του ειδικού επιστήμονα, γίνεται η εγκατάσταση όλων των απαραίτητων εργαλείων, μηχανισμών και αυτοματισμών που σύμφωνα με τις απαιτήσεις μιας Δικανική έρευνας, θα συλλεχτούν και θα παρουσιαστούν όλα τα απαραίτητα δεδομένα τα οποία θα είναι επαρκή για να υποδείξουν τους υπαίτιους μιας ψηφιακής επίθεσης.

Τα proactive εργαλεία που θα χρησιμοποιηθούνε αφορούν τις κινήσεις δικτύου όπως IDS συστήματα και IR μηχανισμούς. Όσον αφορά την εποπτεία των υπηρεσιών ιστού, η μεθοδολογία προτείνει την διαμεσολάβηση ενός τρίτου έμπιστου διαμεσολαβητή (Trusted Third Party), ο οποίος θα αναλαμβάνει να ελέγχει τα transactions μεταξύ των εμπλεκομένων μερών δύο ή περισσοτέρων υπηρεσιών ιστού. Τα εργαλεία αυτά θα πρέπει να είναι αυτόνομα και με όσο το λιγότερο ανθρώπινη παρέμβαση.

Τέταρτο βήμα: Αναγκαία είναι η ύπαρξη πλάνου διαχείρισης το οποίο θα καθορίζει τις αρμοδιότητες των εξωτερικών εγκληματολογικών ερευνητών.

Πέμπτο βήμα: Έγγραφή επικύρωση των διαδικασιών που θα ακολουθούνται κατά την διάρκεια μιας έρευνας.

Φάση 2

Η δεύτερη φάση της βέλτιστης μεθοδολογίας επικεντρώνεται στον εντοπισμό, τη διατήρηση και συλλογή όλων των ψηφιακών αποδεικτικών στοιχείων που θα διευκολύνουν στην διαλεύκανση μιας Δικανικής ψηφιακής έρευνας.

Πρώτο βήμα: Στο πρώτο βήμα της μεθοδολογίας θα πρέπει να αντιμετωπιστεί το περιστατικό της επίθεσης και γίνει επιβεβαίωση ότι τα πληροφορικά συστήματα του οργανισμού έχουν δεχθεί επίθεση. Αν ανιχνευτεί συμβάν επίθεσης θα πρέπει να γίνει αναφορά του περιστατικού και να

απομονωθεί το περιβάλλον του πληροφοριακού περιβάλλοντος που δέχθηκε την επίθεση. Στη συνέχεια θα πρέπει να εφαρμοστεί το πλάνο της έρευνας σύμφωνα με το είδος της επίθεσης και να κατανεμηθούν οι πόροι και οι αρμοδιότητες έτσι ώστε να ξεκινήσει οι συλλογή των πειστηρίων.

Δεύτερο βήμα: Κατά το δεύτερο βήμα θα πρέπει να εντοπιστεί το είδος της επίθεσης , δηλαδή εάν η ψηφιακή επίθεση πλήττει τα «ζωντανά» (live) πληροφοριακά συστήματα του οργανισμού όπως είναι οι υπηρεσίες ιστού ή κινήσεις στο δίκτυο του οργανισμού ή η επίθεση αφορά το file system της εταιρείας.

Στην περίπτωση που ένα πληροφοριακό σύστημα έχει δεχθεί επίθεση στις υπηρεσίες ιστού του ή διαφορετικά στις live υπηρεσίες του, τα συστήματα πέφτουν σε κατάσταση αδρανοποίησης έτσι ώστε να ελαχιστοποιηθούν οι επιπτώσεις στα πληροφοριακά συστήματα ενός οργανισμού σε ένα περιστατικό που βρίσκεται σε εξέλιξη.

Τρίτο βήμα: Στο εν λόγω βήμα γίνεται η συλλογή των πειστηρίων με τα κατάλληλα τεχνολογικά εργαλεία, η τεκμηρίωση τους ότι αποτελούν «αυθεντικά» αποδεικτικά στοιχεία και η φύλαξη τους σε μια λίστα «εξαγόμενων δεδομένων».

Τέταρτο βήμα: Στο τέταρτο βήμα, γίνεται η ανάλυση των δεδομένων που έχουν συλλεχθεί στην προηγούμενη διαδικασία. Αν τα στοιχεία αυτά είναι σχετικά με το συμβάν της επίθεσης και θα βοηθήσουν στην ανακατασκευή του συμβάντος της ψηφιακής επίθεσης, τότε τοποθετούνται στην λίστα των «σχετικών δεδομένων». Αν κατά την διάρκεια της ανάλυσης των δεδομένων προκύψουν νέα δεδομένα τότε αυτά επανεξετάζονται και τοποθετούνται στη κατάλληλη λίστα αν δηλαδή σχετίζονται με το συμβάν της επίθεσης ή δεν αποτελούν πειστήρια.

Πέμπτο βήμα: Σύμφωνα με τις διαδικασίες του πέμπτου βήματος γίνεται προσπάθεια ανακατασκευής του συμβάντος της επίθεσης βάσει των αποδεικτικών στοιχείων που έχουν συλλεχτεί έως εκείνη την στιγμή.

Αν η επίθεση αφορά υπηρεσίες ιστού και όλοι οι αυτοματισμοί και τα εργαλεία που έχουν εγκατασταθεί και προβλεφτεί κατά την πρώτη φάση (Proactive) έχουν καταγράψει όλες τις απαραίτητες πληροφορίες, θα πρέπει να βρεθεί ένα σημείο εκκίνησης του συμβάντος. Τα Δικανικά εργαλεία των υπηρεσιών ιστού που αναλαμβάνουν να καταγράψουν τα «ζωντανά» δεδομένα που συναλλάσσονται θα πρέπει να περιλαμβάνουν:

- Αποδεικτικά στοιχεία προέλευσης, τα οποία περιλαμβάνουν την ώρα που αποστάλθηκε ένα μήνυμα.
- Αποδεικτικά στοιχεία παράδοσης, στο οποίο περιλαμβάνεται το μήνυμα αποδοχής από το παραλήπτη και τη χρονική στιγμή που παραλήφτηκε.
- Τα στοιχεία του χρήστη της υπηρεσίας ιστού, τα οποία μπορεί να περιλαμβάνουν το όνομα χρήστη, την ώρα που εισήχθη για να χρησιμοποιήσει την υπηρεσία κ.α.
- Αρχεία καταγραφής τα οποία ανιχνεύουν το είδος της επίθεσης και τις ευπάθειες ενός πληροφοριακού συστήματος.
- Εργαλεία που συλλέγουν αποδεικτικά στοιχεία παραβίασης και κινήσεις στο δίκτυο και τις υπηρεσίες των πληροφοριακών συστημάτων του οργανισμού.

Έκτο βήμα: Στην περίπτωση που τα αποδεικτικά στοιχεία δεν επαρκούν για την ανακατασκευή του συμβάντος της επίθεσης τότε η διαδικασία θα πρέπει να επαναληφθεί από το τρίτο βήμα της δεύτερης φάσης έως ότου τα δεδομένα θα κριθούν επαρκή για το τερματισμό της Δικανικής έρευνας.

Φάση 3

Στην τρίτη και τελευταία φάση της βέλτιστης μεθοδολογίας, εκτελούνται όλες οι απαραίτητες διαδικασίες για τον τερματισμό της εγκληματολογικής έρευνας.

Πρώτο βήμα: Στο πρώτο βήμα της τρίτης φάσης, θα πρέπει να αξιολογηθούν τα εναπομείναντα δεδομένα αν αποτελούν πειστήρια της δραστικής ψηφιακής εγκληματολογίας έτσι ώστε να εκτελεστούν τα κατάλληλα βήματα για την ανάλυση τους και την ανακατασκευή ενός συμβάντος ψηφιακής επίθεσης όπως αυτό έχει περιγραφεί στην δεύτερη φάση της μεθοδολογίας και αναλόγως επαναλαμβάνονται τα βήματα που εφαρμόζονται και στην ενεργή ψηφιακή εγκληματολογία.

Δεύτερο βήμα: Κατά το δεύτερο βήμα γίνεται η αποκατάσταση των συστημάτων και όλων των υπηρεσιών του οργανισμού έτσι ώστε να συνεχισθεί η επιχειρησιακή συνέχεια το ταχύτερο δυνατό.

Τρίτο βήμα: Στο τρίτο βήμα οι ειδικοί εγκληματολόγοι της Δικανικής έρευνας παγιώνουν τα αποτελέσματα της έρευνας και στη συνέχεια παραθέτουν μια τεκμηριωμένη έκθεση με όλα τα πειστήρια της ψηφιακής έρευνας που συμμετέχουν στην επίλυση της υπόθεσης.

Τέταρτο βήμα: Στο συγκεκριμένο και τελευταίο βήμα της $3^{ης}$ φάσης, γίνεται η παρουσίαση των ευρημάτων όλων των προηγουμένων φάσεων στις δικαστικές αρχές. Παρουσιάζεται βάση των νομικών πλαισίων όλο το χρονοδιάγραμμα της επίθεσης και τα πειστήρια που τα οποία υποστηρίζουν ότι ένα ψηφιακό περιβάλλον δέχθηκε κακόβουλη επίθεση. Τέλος γίνεται η ανακοίνωση των αποτελεσμάτων από τις δικαστικές αρχές και το κλείσιμο της υπόθεσης.

Στο κεφάλαιο που ακολουθεί θα γίνει εφαρμογή του πλαισίου της βέλτιστης μεθοδολογίας το οποίο περιγράφτηκε στις προηγούμενες ενότητες στηριζόμενο σε ένα παράδειγμα ψηφιακής επίθεσης που προσομοιάζει ένα «ζωντανό» τεχνολογικό περιβάλλον ενός οργανισμού.

4 Πρακτικό μέρος

Στο 4ο μέρος της μεταπτυχιακής εργασίας, θα γίνει εφαρμογή της βέλτιστης μεθοδολογίας που παρουσιάστηκε στην ενότητα 3.2 . Στη συνέχεια θα γίνει παρουσίαση του περιβάλλοντος που θα διεξαχθεί μια προσομοίωση πραγματικού σεναρίου. Θα γίνει αναλυτική επεξήγηση όλων των βασικών εννοιών που συναντώνται κατά την πειραματική διαδικασία έτσι ώστε να γίνει κατανοητό κάθε βήμα της πειραματικής διαδικασίας.

Στην ενότητα που θα ακολουθήσει (4.2), θα γίνει η περιγραφή του προβλήματος και πώς τα αποτελέσματα αυτού θα μας εμπόδιζαν στο να διεξαχθεί μια αποτελεσματική Δικανική έρευνα. Στη συνέχεια θα προταθούν τα αντίμετρα τα οποία θα επέτρεπαν την διεξαγωγή μιας ομαλής συλλογής όλων των πειστηρίων της επίθεσης σύμφωνα με τις διαδικασίες της βέλτιστης μεθοδολογίας που έχει προταθεί.

Στην ενότητα 4.3 θα γίνει αναλυτική περιγραφή των εργαλείων που θα χρησιμοποιηθούν και θα γίνει η διεξαγωγή του πειράματος σύμφωνα με την μεθοδολογία της ενότητας 3.2.

Τέλος, θα γίνει η αξιολόγηση των αποτελεσμάτων της πειραματικής διαδικασίας και θα εξαχθούν συμπεράσματα για την αποτελεσματικότητα της εφαρμογής των τεχνολογικών εργαλείων σε συνδυασμό με την περιγραφείσα μεθοδολογία.

4.1 Ανάλυση πειραματικού περιβάλλοντος

Στην παρούσα ενότητα θα αναλυθεί το περιβάλλον που θα διεξαχθούν οι πειραματικές διαδικασίες. Θα γίνει προσπάθεια προσέγγισης και προσομοίωσης συμβάντων επιθέσεων τα οποία απαντώνται σε πραγματικά περιβάλλοντα διαφόρων οργανισμών και πρέπει να αντιμετωπιστούν με τις κατάλληλες τεχνολογίες και μεθόδους.

Όπως έχει προαναφερθεί στις προηγούμενες ενότητες η αντιμετώπιση επιθέσεων σε υπηρεσίες ιστού αποτελούν μια μεγάλη πρόκληση λόγω της πολυπλοκότητας που παρουσιάζουν και τις δυσκολίας ελέγχου των συναλλαγών τους όταν εμπλέκονται πολλές υπηρεσίες ιστού (web services) ταυτόχρονα. Ακόμα η συλλογή πληροφοριών οι οποίες θα έχουν Δικανική αξία, αποτελεί άλλο ένα στόχο της Δικανικής πληροφορικής που εφαρμόζεται στις υπηρεσίες ιστού. Πολλοί οργανισμοί και εταιρείες ολοένα ενσωματώνουν υπηρεσίες ιστού στο περιβάλλον τους, για ενδοεταιρικούς σκοπούς ή για εξυπηρέτηση διάφορων χρηστών εκτός του περιβάλλοντος του οργανισμού. Παράδειγμα αποτελεί η χρήση web υπηρεσιών ενός ιστοτόπου που παρέχει υπηρεσίες ηλεκτρονικού καταστήματος, όταν ένας χρήστης επιθυμεί να πληρώσει τα προϊόντα που έχει επιλέξει μέσω πιστωτικής κάρτας μια ή περισσότερες υπηρεσίες ιστού οι οποίες έχουν περάσει τους κατάλληλους ελέγχους αξιοπιστίας μεταξύ τους, ανάμεσα στο ηλεκτρονικό κατάστημα και την τράπεζα, αναλαμβάνει να πιστοποιήσει τα στοιχεία της κάρτας του αγοραστή έτσι ώστε να ολοκληρωθεί με ασφάλεια η διαδικασία της παραγγελίας του προϊόντος.

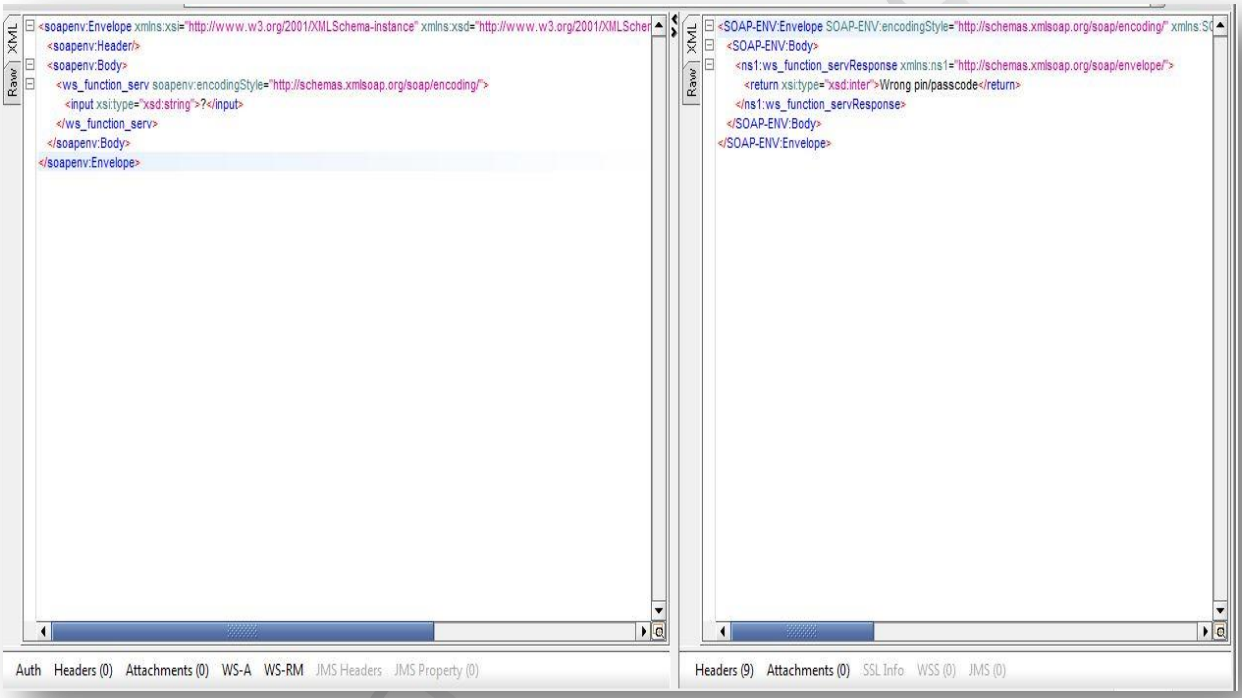
Οι υπηρεσίες ιστού μπορούν εύκολα να εφαρμοστούν με διάφορες γλώσσες προγραμματισμού. Στην παρούσα μεταπτυχιακή διατριβή θα γίνει αναφορά και πειραματική έρευνα με τη χρήση υπηρεσιών ιστού στην γλώσσα προγραμματισμού PHP[24] . Στο σημείο αυτό θα πρέπει να γίνει αναφορά σε θεμελιώδεις έννοιες που θα βοηθήσουν στην κατανόηση του προβλήματος σε βάθος και για το πώς αυτές εφαρμόστηκαν κατά την πειραματική διαδικασία.

Δύο τύποι υπηρεσιών που έχουν συναφή στοιχεία είναι οι υπηρεσίες κλήσης απομακρυσμένων διαδικασιών (RPC) και οι υπηρεσίες SOAP (έχει γίνει αναφορά των SOAP μηνυμάτων στην ενότητα 3.1.3 μεθοδολογία των Web Services). Οι δύο αυτές υπηρεσίες έχουν παρόμοια χαρακτηριστικά καθώς και οι δύο περιλαμβάνουν λειτουργίες κλήσης και διαβιβάζουν παραμέτρους. Η μεγαλύτερη διαφορά τους είναι ότι οι υπηρεσίες SOAP είναι πιο αυστηρά καθορισμένες από αυτές της κλήσης απομακρυσμένων διαδικασιών (RPC). Το RPC είναι ένα πρωτόκολλο κατά το οποίο ένα πρόγραμμα μπορεί να χρησιμοποιήσει για να ζητήσει μια υπηρεσία από ένα άλλο πρόγραμμα που βρίσκεται σε έναν άλλο υπολογιστή σε ένα ξεχωριστό, δίκτυο χωρίς να χρειάζεται να γίνουν κατανοητές οι λεπτομέρειες του δικτύου αυτού. Το RPC χρησιμοποιεί το μοντέλο πελάτη – εξυπηρετητή (client / server). Το πρόγραμμα πελάτης (client) κάνει την αίτηση προς το πρόγραμμα παροχής υπηρεσιών που έχει το ρόλο του διακομιστή. Το RPC καλύπτει το στρώμα μεταφοράς και το στρώμα εφαρμογής του μοντέλου διασύνδεσης ανοικτών συστημάτων (OSI), μιας διαδικτυακής επικοινωνίας. Το RPC καθιστά ευκολότερο να αναπτυχτεί μια εφαρμογή που περιλαμβάνει πολλά προγράμματα που διανέμονται σε ένα δίκτυο.

Το SOAP βασίζεται στη XML γλώσσα προγραμματισμού και αποτελεί ένα πρωτόκολλο που μας δίνει την δυνατότητα πρόσβασης σε μια υπηρεσία ιστού. Σαν XML πρωτόκολλο επιτρέπει στις εφαρμογές να ανταλλάσσουν πληροφορίες πάνω από το HTTP πρωτόκολλο. Το SOAP είναι μια υπηρεσία όμοια με αυτή του RPC αλλά με μια συγκεκριμένη δομή μορφής XML. Το SOAP

[24] Η PHP είναι μια σεναριακή γλώσσα προγραμματισμού (Script Programming Language). Είναι κατάλληλη για την ανάπτυξη διαδικτυακών εφαρμογών και προγραμματιδίων συστήματος (System Scripts).

επιτρέπει την δημιουργία διαλειτουργικών λογισμικών και επιτρέπει σε διάφορους χρήστες να επωφεληθούν από τις υπηρεσίες ενός λογισμικού μέσω διαδικτύου. Ορίζει τους κανόνες για την αποστολή και λήψη των υπηρεσιών κλήσης των απομακρυσμένων διαδικασιών (RPC), όπως τη δομή της αίτησης και την δομή των απαντήσεων. Ως εκ τούτου, το SOAP δεν συνδέεται με οποιοδήποτε συγκεκριμένο λειτουργικό σύστημα ή γλώσσα προγραμματισμού. Στη παρακάτω εικόνα εμφανίζεται η δομή ενός SOAP μηνύματος καθώς και η παραγόμενη απάντηση από τον εξυπηρετητή σε XML μορφή.



Εικόνα 17. Παραγόμενο SOAP μηνύματος πελάτη- εξυπηρετητή σε μορφή XML από το πρόγραμμα SoapUI.

Το SOAP τέλος, ενσωματώνει τις τεχνικές και τις διαδικασίες του WSDL σχήματος και μπορεί να χρησιμοποιηθεί πολύ εύκολα με την γλώσσα προγραμματισμού PHP καθώς παρουσιάζει ένα μεγάλο σύνολο βιβλιοθηκών τόσο για τον πελάτη (client) όσο και για τον διακομιστή (server).

Η γλώσσα WSDL (Web Service Description Language), αποτελεί ένα σχήμα XML για την περιγραφή δικτυακών υπηρεσιών. Παρέχει την δυνατότητα να περιγραφούν αιτήσεις και απαντήσεις διαφόρων υπηρεσιών ιστού πάνω από διαφορετικά πρωτόκολλα και τύπους κωδικοποιήσεων. Γενικότερα θα μπορούσαμε να πούμε ότι η γλώσσα WSDL στην περιγραφή ενός συνόλου μηνυμάτων και για το πώς αυτά ανταλλάσσονται. Το XML σχήμα που χρησιμοποιεί την καθιστά ανεξάρτητη από τις διάφορες γλώσσες προγραμματισμού και μπορεί να περιγράψει εύκολα διάφορε υπηρεσίες ιστού. Η WSDL είναι εύκολα επεκτάσιμη στο να επιτρέπει την περιγραφή μηνυμάτων άσχετα από τη μορφή των πρωτοκόλλων δικτύων που χρησιμοποιούνται για την επικοινωνία. Η WSDL χρησιμοποιείται για να περιγράψει τί μπορεί να κάνει ένα web service, για το πού βρίσκεται και για το πώς μπορεί κάποιος να το καλέσει. Η WSDL ορίζει υπηρεσίες σαν συλλογές από τελικά σημεία δικτύου ή αλλιώς ports. Στην WSDL ο περιγραφικός

ορισμός των τελικών σημείων και των μηνυμάτων διαχωρίζεται από συγκεκριμένα δικτυακά πρωτόκολλα ή μορφές δεδομένων. Ένα έγγραφο WSDL χρησιμοποιεί τα στοιχεία που ακολουθούν για τον ορισμό δικτυακών υπηρεσιών :

1. **Τύπους (Types)**. Τύπους δεδομένων όπως για παράδειγμα το XML σχήμα.
2. **Μηνύματα** τα οποία αποτελούν τα δεδομένα που ανταλλάσσονται.
3. **Λειτουργίες**. Όπου δίνεται η περιγραφή λειτουργίας μιας υπηρεσίας ιστού.
4. **Τύπος πόρτας (Port Type)**. Περιγράφει το σύνολο από λειτουργίες που υποστηρίζονται από ένα ή περισσότερα τελικά σημεία.
5. **Πρωτόκολλο σύνδεσης (Binding)**.Αποτελεί το πρωτόκολλο και την μορφή των δεδομένων για ένα συγκεκριμένο τύπο πόρτας (port type).
6. **Πόρτα (port)**. Καθορίζει τελικό σημείο που ορίζεται σαν συνδυασμός μίας σύνδεσης (binding) και μιας διεύθυνσης δικτύου.
7. **Υπηρεσία.** Είναι το σύνολο από τα διάφορα τελικά σημεία των υπηρεσιών ιστού που συναλλάσσονται.

Στην εικόνα που ακολουθεί εμφανίζεται η XML δομή ενός WSDL εγγράφου.

```
- <definitions targetNamespace="urn:demo">
  - <types>
    - <xsd:schema targetNamespace="urn:demo">
        <xsd:import namespace="http://schemas.xmlsoap.org/soap/encoding/"/>
        <xsd:import namespace="http://schemas.xmlsoap.org/wsdl/"/>
      </xsd:schema>
    </types>
  - <message name="ws_function_servRequest">
      <part name="input" type="xsd:string"/>
    </message>
  - <message name="ws_function_servResponse">
      <part name="return" type="xsd:inter"/>
    </message>
  - <portType name="demoPortType">
    - <operation name="ws_function_serv">
        <input message="tns:ws_function_servRequest"/>
        <output message="tns:ws_function_servResponse"/>
      </operation>
    </portType>
  - <binding name="demoBinding" type="tns:demoPortType">
      <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
    - <operation name="ws_function_serv">
        <soap:operation soapAction="http://192.168.0.20/soap_ws2/service.php/ws_function_serv" style="rpc"/>
      - <input>
          <soap:body use="encoded" namespace="" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
        </input>
      - <output>
          <soap:body use="encoded" namespace="" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
        </output>
      </operation>
    </binding>
  - <service name="demo">
    - <port name="demoPort" binding="tns:demoBinding">
        <soap:address location="http://192.168.0.20/soap_ws2/service.php"/>
      </port>
    </service>
</definitions>
```

Εικόνα 18. WSDL αρχείο στο XML σχήμα του.

Η γλώσσα PHP μπορεί να χρησιμοποιηθεί με μεγάλη ευκολία συνδυαστικά με το SOAP κάνοντας χρήση της βιβλιοθήκης NuSOAP. Παρέχει ένα απλό αντικειμενοστραφές περιβάλλον (object – oriented) και μπορεί να παράγει αυτόματα WSDL αρχεία για μια υπηρεσία. Στην ενότητα 4.3 θα γίνει αναλυτική περιγραφή υλοποίησης υπηρεσίας που βασίζεται σε γλώσσα PHP και SOAP μηνύματα κάνοντας χρήση της βιβλιοθήκης NuSoap. Στην παρακάτω εικόνα εμφανίζεται ο κώδικας μιας client υπηρεσίας ο οποίος περιλαμβάνει την εισαγωγή της βιβλιοθήκης NuSOAP τον προσδιορισμό του και την δημιουργία του client, το URL του τελικού σημείου (endpoint) της υπηρεσίας ιστού και τη δημιουργία του WSDL αρχείου. Τέλος, καλείται η λειτουργία της υπηρεσίας και εμφανίζονται τα αποτελέσματα.

```php
<?php
    //include soap library
    require 'lib/nusoap.php';
    //define soap client with SERVICE ws
    $client = new nusoap_client("http://localhost/soap_ws1/service.php?wsdl");

    //call SERVICE ws function, send parameters, get result
    $balance = $client->call('ws_function_serv', $params);

    //got the result from SERVICE
    //result can be anything (single value or array of values)
    //on this example the result is just a number (balance of the user's account)
    //display result
    echo "Balance = ".$balance."<br><br><br>";
}?>
```

Εικόνα 19. Κώδικας client υπηρεσίας.

Στην επόμενη εικόνα εμφανίζεται η δημιουργία ενός SOAP εξυπηρετητή. Ο προσδιορισμός της λειτουργίας της υπηρεσίας και η δημιουργία ενός HTTP ακροατή (listener) που καλεί την υπηρεσία.

```php
<?php
require 'lib/nusoap.php';
$server = new nusoap_server(); // Create server instance
$server->configureWSDL('demo',"urn:demo");
$server->register("ws_function_serv"); //identify the service function

// create HTTP listener invoke the service
$HTTP_RAW_POST_DATA = isset($HTTP_RAW_POST_DATA) ? $HTTP_RAW_POST_DATA : '';
$server ->service($HTTP_RAW_POST_DATA);
?>
```

Εικόνα 20. Δημιουργία SOAP εξυπηρετητή.

4.2 Περιγραφή προβλήματος

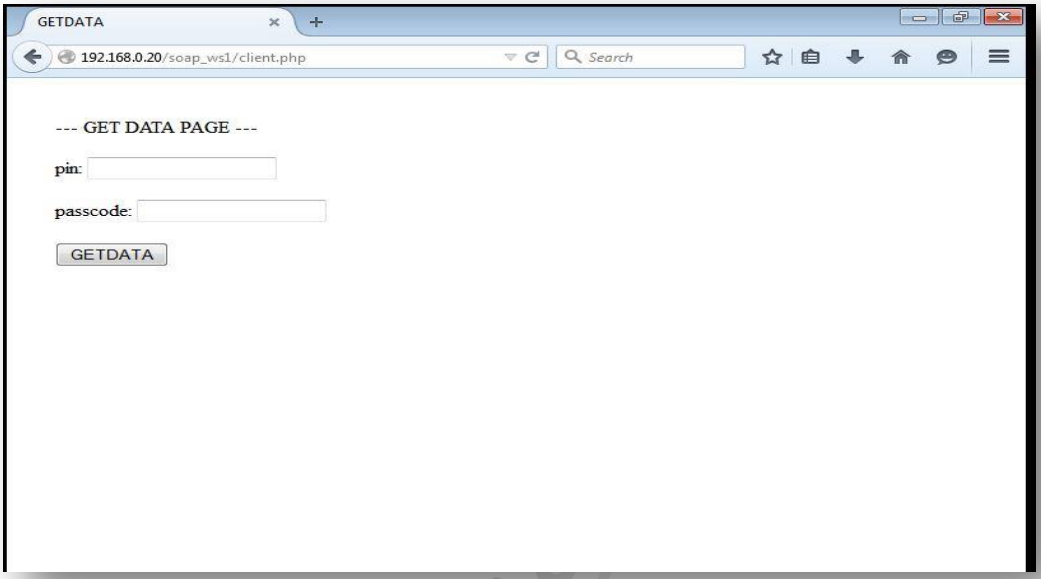
Στην παρούσα μεταπτυχιακή διατριβή θα παρουσιαστούν παραδείγματα τα οποία προσημειώνουν λειτουργίες ενός πραγματικού τεχνολογικού περιβάλλοντος σε ένα οργανισμό ή επιχείρηση. Θα δοθεί ιδιαίτερη βαρύτητα στην λειτουργία των υπηρεσιών ιστού για το πώς αυτές μπορούν να προστατευτούν, με ποια εργαλεία και με ποιες τεχνικές και μεθόδους μπορούν να συλλεχθούν και να αναλυθούν δεδομένα τα οποία θα αποτελέσουν πειστήρια σε μια ενδεχόμενη Δικανική έρευνα.

Στην ενότητα που ακολουθεί (4.3) θα γίνει παρουσίαση ενός περιβάλλοντος στο οποίο με τη χρήση υπηρεσιών ιστού ανταλλάζονται XMLμηνύματα μεταξύ του πελάτη και του εξυπηρετητή και επιστρέφονται τα ανάλογα αποτελέσματα. Ιδιαίτερη αναφορά θα γίνει στη χρησιμότητα ενός διακομιστή που θα λειτουργεί σαν «έμπιστο» ενδιάμεσο εργαλείο (Trusted Third Party server) που θα ελέγχει την κίνηση και την ανταλλαγή μηνυμάτων μεταξύ των προγραμμάτων πελάτη και εξυπηρετητή. Αναλυτικότερα θα γίνει παρουσίαση τριών εκδοχών ενός online συστήματος τραπέζης στο οποίο ο χρήστης αφού συνδεθεί με τα έγκυρα στοιχεία του που υπάρχουν στην βάση, θα έχει την δυνατότητα βάζοντας τα προσωπικά του μοναδικά δεδομένα «pin» και «passcode» να του επιστρέφεται το υπόλοιπο του λογαριασμού του. Στο σύστημα έχουν δημιουργηθεί εσκεμμένα κενά ασφαλείας έτσι ώστε να αποδειχθεί η χρησιμότητα των εργαλείων της Δικανικής και αποτελεσματικότητα της βέλτιστης μεθοδολογίας όπως αυτή έχει περιγραφτεί στην ενότητα 3.2.4.

Συγκεκριμένα θα παρουσιαστούν τα ακόλουθα σενάρια:

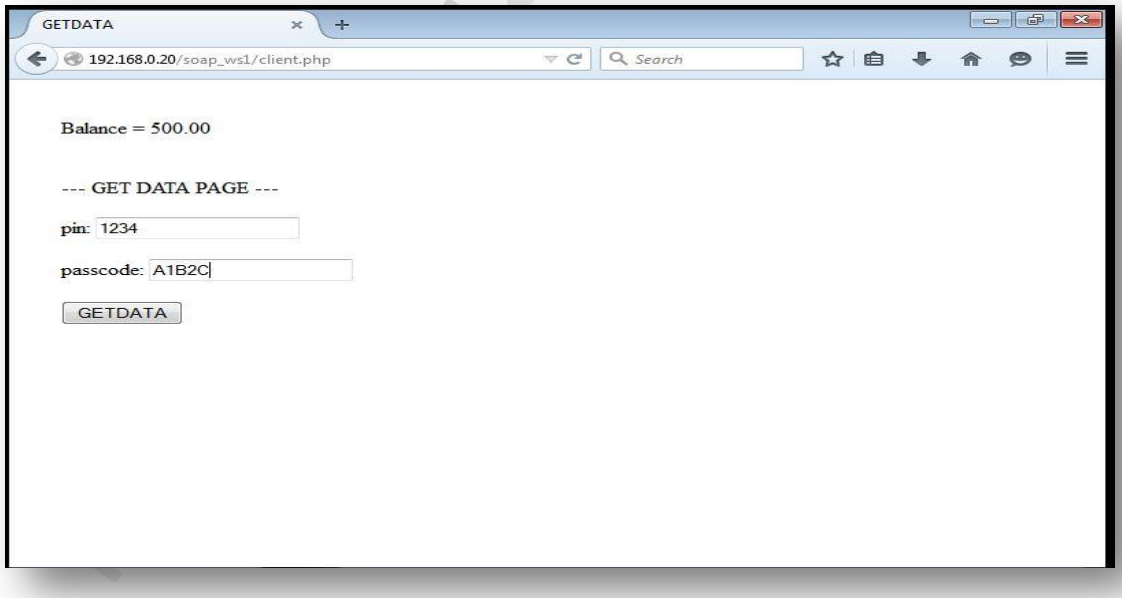
1. Στην πρώτη περίπτωση παρουσιάζεται πειραματικά η απλούστερη μορφή που μπορεί να έχει μια υπηρεσία ιστού ενός οργανισμού. Κατά τη λειτουργία της υπηρεσίας ένας χρήστης, συμπληρώνοντας αρχικά σωστά τα διαπιστευτήρια του έχει την δυνατότητα να εισαχθεί στο σύστημα και στη συνέχεια συμπληρώνοντας δύο παραμέτρους, μοναδικές για κάθε χρήστη «pin» και «passcode», όπως αυτά εμφανίζονται στην εικόνα που

ακολουθεί.



Εικόνα 21. Σελίδα εισαγωγής «pin» και «passcode» χρήστη.

Αν ο χρήστης συμπληρώσει τα πεδία με τα μοναδικά του στοιχεία τότε του επιστρέφεται το υπόλοιπο του λογαριασμού του.



Εικόνα 22. Σελίδα επιστροφής υπολοίπου του χρήστη.

Στο πρώτο σενάριο, με τα κατάλληλα εργαλεία θα εφαρμοστούν επιθέσεις τύπου άρνησης υπηρεσιών (DOS attacks), Sql Injection και με το εργαλείο SoapUI (η λειτουργία του θα παρουσιαστεί αναλυτικότερα στην επόμενη ενότητα). Οι επιθέσεις άρνησης υπηρεσιών έχουν

σαν κύριο σκοπό να καταστήσουν ανίκανη μια υπηρεσία που παρέχεται από ένα οργανισμό ή ένα εξυπηρετητή, στο να εξυπηρετήσει αιτήσεις χρηστών και πελατών. Το δεύτερο είδος επίθεσης (Sql injection), αναφέρεται σε μια ευπάθεια που συναντάται σε βάσεις δεδομένων κατά την οποία ανεπιθύμητοι χαρακτήρες μπορούν να περάσουν σαν ερωτήματα sql προς την βάση δεδομένων ενός οργανισμού και ένας κακόβουλος χρήστης να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες που μπορεί να αφορούν προσωπικά δεδομένα χρηστών ή οικονομικά στοιχεία μια εταιρείας. Τέλος, στο πρώτο σενάριο θα αποδειχθεί ότι οι πληροφορίες που μπορούν να συλλεχθούν σε ένα τέτοιο περιβάλλον και αυτού του τύπου επιθέσεων δεν έχουν εγκληματολογική αξία σε μια Δικανική έρευνα.

2. Στη δεύτερη πειραματική υλοποίηση θα παρουσιαστεί και θα αναλυθεί ο τρόπος λειτουργίας ενός ενδιάμεσου εξυπηρετητή ο οποίους θα λαμβάνεται σαν μια τρίτη ξεχωριστή έμπιστη οντότητα (Trusted Third Party) από τις υπηρεσίες ιστού, η οποία θα εποπτεύει τις συναλλαγές μεταξύ των υπηρεσιών των προγραμμάτων πελάτη και διακομιστή. Ο κύριος ρόλος του TTP είναι στο να έχει το ρόλο του διαμεσολαβητή μεταξύ των υπηρεσιών πελάτη και των υπηρεσιών του εξυπηρετητή, διαβιβάζοντας τα μηνύματα του ενός προς τον άλλο με ασφαλή τρόπο και εποπτεύοντας με την χρήση αρχείων καταγραφής (log files) την μεταξύ τους λειτουργία. Ακόμα θα γίνει χρήση επιπρόσθετων εργαλείων (modules) τα οποία θα συνεισφέρουν στη συλλογή δεδομένων κατά την διάρκεια μιας εγκληματολογικής έρευνας και πολλές φορές θα αποτρέπουν και θα προλαμβάνουν κακόβουλες επιθέσεις. Θα παρουσιαστούν τα στοιχεία που μπορούν να συλλεχθούν αλλά με τη χρήση του εργαλείο SoapUI θα αποδειχθεί ότι παρόλα τα μέτρα που έχουν ληφθεί κάποιες επιθέσεις δεν μπορούν ανιχνευτούν.
3. Στο τρίτο σενάριο θα παρουσιαστεί και θα εφαρμοστεί μια ολοκληρωμένη λύση ως προς την αντιμετώπιση επιθέσεων σε υπηρεσίες ιστού. Θα καλυφτούν με τις κατάλληλες τεχνικές και εργαλεία όλες οι ελλείψεις που παρουσιάστηκαν στα δύο προηγούμενα σενάρια. Επιπροσθέτως στη τελευταία υλοποίηση θα γίνει η χρήση και εφαρμογή των βημάτων τις βέλτιστης μεθοδολογίας όπως αυτή περιγράφτηκε στις προηγούμενες ενότητες. Θα εξαχθούν και θα αναλυθούν όλα τα απαραίτητα αποδεικτικά στοιχεία που θα επιτρέψουν την διαλεύκανση της ψηφιακής επίθεσης που δέχθηκαν οι υπηρεσίες ιστού του πειραματικού περιβάλλοντος που θα παρουσιαστεί στην ενότητα 4.3.

Τέλος θα αξιολογηθούν τα αποτελέσματα των τριών σεναρίων καθώς και η αποτελεσματικότητα της βέλτιστης μεθοδολογίας που εφαρμόστηκε (ενότητα 4.4).

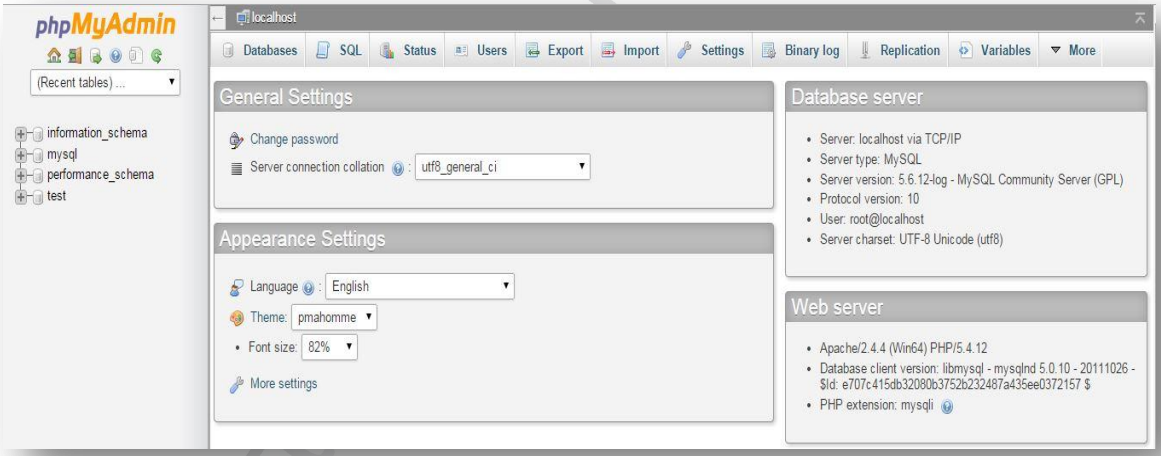
4.3 Περιγραφή των εργαλείων – Πειραματικό μέρος

Στην ενότητα 4.3 θα γίνει αναλυτική παρουσίαση όλων των τεχνολογικών εργαλείων που θα πάρουν μέρος στο εργαστηριακό κομμάτι. Θα ακολουθήσει η βήμα προς βήμα επεξήγηση του τεχνολογικού περιβάλλοντος, η λειτουργία των υπηρεσιών που λαμβάνουν μέρος σε κάθε περίπτωση καθώς και πως αυτά υλοποιήθηκαν. Ακόμα στο τελευταίο σενάριο του πειραματικού μέρους θα γίνει η εφαρμογή της βέλτιστης Δικανικής μεθοδολογίας και των βημάτων της και θα παρουσιαστούν τα δεδομένα και τα πειστήρια της ψηφιακής επίθεσης. Τέλος, θα πρέπει να τονιστεί ότι το πρακτικό μέρος που παρουσιάζεται εστιάζει στην αντιμετώπιση συμβάντων επίθεσης ενάντια σε υπηρεσίες ιστού ενός τεχνολογικού περιβάλλοντος και στην συλλογή αποδεικτικών στοιχείων με εγκληματολογική αξία.

Στην παρούσα παράγραφο θα παρουσιαστούν τα βασικά εργαλεία που χρησιμοποιούνται για το σχεδιασμό του πειραματικού περιβάλλοντος καθώς και τα εργαλεία τα οποία περιλαμβάνουν τεχνικές επιθέσεων τις οποίες τις συναντάμε και σε πραγματικές συνθήκες ψηφιακών επιθέσεων.

Για τη διεξαγωγή του πειραματικού μέρους πραγματοποιήθηκαν εικονικά περιβάλλοντα τα οποία επικοινωνούν κάτω από ένα εικονικό (virtual) δίκτυο. Στα παραδείγματα που θα παρουσιαστούν θα λάβουν μέρος τρείς οντότητες υπηρεσιών ιστού: υπηρεσία πελάτης – εξυπηρετητής, υπηρεσία έμπιστης τρίτης οντότητας (Trusted Third Party). Σε όλα τα παραδείγματα που θα υλοποιηθούν παρουσιάζεται μια διαδικτυακή υπηρεσία ηλεκτρονικής τραπεζικής στην οποία ένα χρήστης θα του δίνεται η δυνατότητα αφού εισαχθεί στο σύστημα με τους κωδικούς του, να κάνει αίτημα προς την βάση της τράπεζας και μέσω ανταλλαγής μηνυμάτων των υπηρεσιών να λάβει την κατάλληλη απάντηση.

Για την δημιουργία των υπηρεσιών χρησιμοποιήθηκε το περιβάλλον WampServer[25]. Το WampServer περιλαμβάνει ένα περιβάλλον ανάπτυξης που μπορεί να χρησιμοποιηθεί από τις διάφορες πλατφόρμες λογισμικού όπως windows, linux κτλ. Επιτρέπει την δημιουργία υπηρεσιών ιστού με χρήση Apache sever , γλώσσα προγραμματισμού PHP και γλώσσα βάσεων δεδομένων MySql. Όποτε ένας χρήστης επιθυμεί να επισκεφτεί μια ιστοσελίδα το πρόγραμμα πλοήγησης (browser) επικοινωνεί με έναν διακομιστή (server) μέσω του πρωτοκόλλου HTTP, ο οποίος παράγει τις ιστοσελίδες και τις αποστέλλει στο πρόγραμμα πλοήγησης, ο Apache HTTP Server (15) αναλαμβάνει τέτοιου είδους επικοινωνίες. Το εργαλείο PHP admin που περιλαμβάνεται στο περιβάλλον WampServer, είναι ένα εργαλείο ανοικτού κώδικα γραμμένο σε γλώσσα PHP το οποίο μας επιτρέπει την διαχείριση βάσεων δεδομένων MySql μέσω ενός φυλλομετρητή ιστού.



Εικόνα 23. Περιβάλλον εργασίας phpmyadmin.

Κατά την διάρκεια των πειραματικών δοκιμών θα γίνει η χρήση του εργαλείου modSecurity (16). Το modSecurity είναι μια τρίτη οντότητα (module), το οποίο συνδυαστικά με τον Apache εξυπηρετητή προσφέρει ανίχνευση και προστασία λειτουργώντας σαν τείχος προστασίας (firewall), αποτρέποντας διαδικτυακές επιθέσεις σε υπηρεσίες ιστού. Το modSecurity παρέχει όλα τα εργαλεία για να αποτρέψει επιθέσεις SQL injection, XSS cross-site scripting, άρνησης υπηρεσιών DoS (DoS attacks), καταχώρησης αρχείων (file inclusion). Το modSecurity προσφέρει προστασία μέσω ενός συνόλου κανόνων (rule set) και οι βασικοί του κανόνες αποτελούν το Core Rule Set (CRS), μερικοί από αυτούς θα παρουσιαστούν στις επόμενες

[25] Πληροφορίες και οδηγίες εκμάθησης για το WampServer βρίσκονται στο παρακάτω σύνδεσμο: http://www.wampserver.com/en/

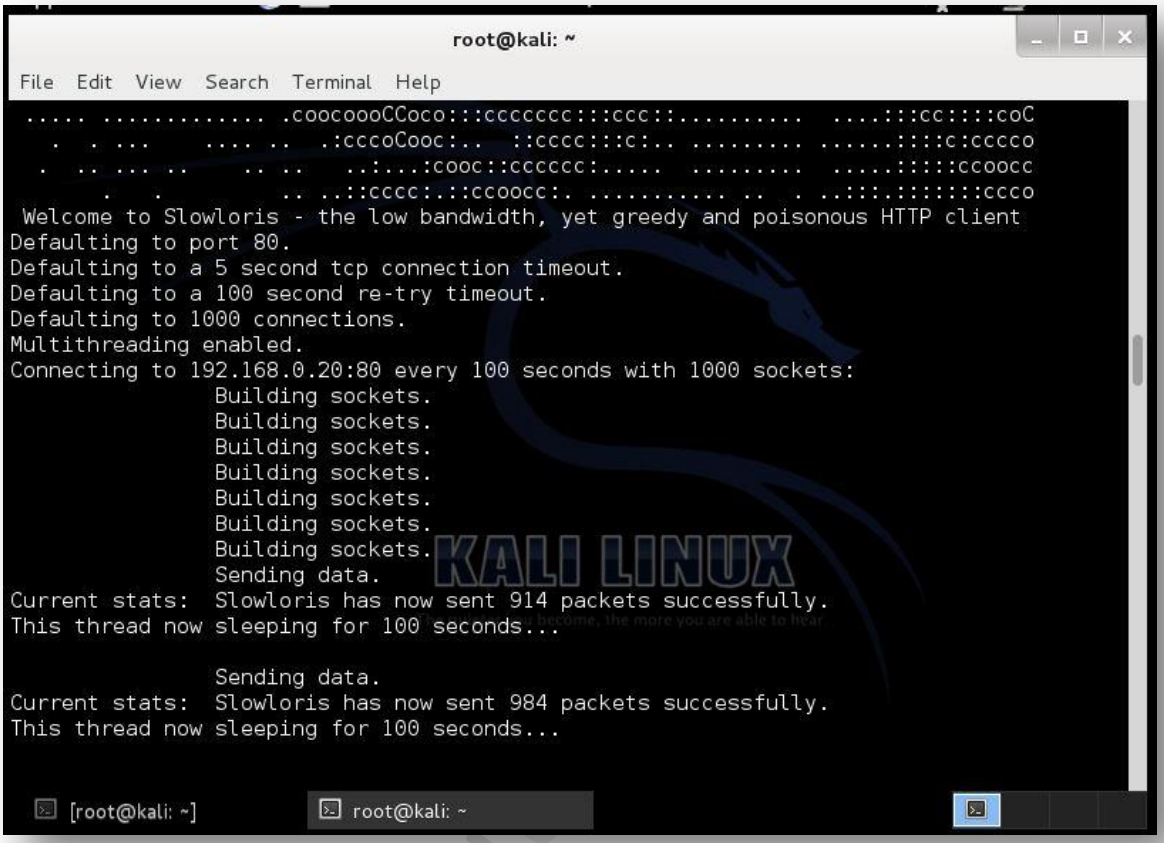
ενότητες. Παρόμοια και συμπληρωματική λειτουργιά με αυτή του modSecurity εμφανίζει και το πρόσθετο module του Apache, mod_antiloris παρέχοντας όμως περισσότερες επιλογές στην αντιμετώπιση HTTP DOS επιθέσεων παρεμποδίζοντας την πρόσβαση σε ένα εξυπηρετητή όταν υπερβαίνουν ένα μέγιστο αριθμό ταυτόχρονων συνδέσεων ή τη φόρτωση της ίδιας σελίδας πολλές φορές σε λίγα δευτερόλεπτα.

Στις επόμενες ενότητες θα γίνει χρήση εργαλείων επίθεσης προς τις υπηρεσίες ιστού που θα υλοποιηθούν. Μέσω της χρήσης εικονικού περιβάλλοντος και του λειτουργικού Kali Linux26 το οποίο αποτελεί μια Debian διανομή και παρέχει ένα σύνολο δωρεάν προγραμμάτων και υπηρεσιών. Το Kali Linux είναι η μετεξέλιξη της διανομής Backtrack και έχει δημιουργηθεί με κύριο σκοπό για χρήση σε δοκιμές επιθέσεων και διεισδύσεων σε ψηφιακά συστήματα. Το εργαλείο που θα χρησιμοποιηθεί μέσω της διανομής ονομάζεται SlowLoris[27]. Το SlowLoris είναι ένα εργαλείο επιθέσεων άρνησης υπηρεσιών (DoS attacks). Η κύρια λειτουργία του είναι να κρατά ανοιχτές συνδέσεις (calls) με ένα εξυπηρετητή αποστέλλοντας HTTP αιτήματα, κατά την διάρκεια της επίθεσης στέλνονται και άλλα αιτήματα ανά τακτά χρονικά διαστήματα έτσι ώστε να εμποδίσει τα υποδοχές (sockets) του εξυπηρετητή να κλείσουν, με αποτέλεσμα οι διακομιστές ιστού να μην μπορούν να εξυπηρετήσουν άλλα αιτήματα. Ειδικότερα, οι διακομιστές που χρησιμοποιούν threads θα τείνουν να είναι πιο ευάλωτοι σε επιθέσεις, λόγω του γεγονότος ότι προσπαθούν να περιορίσουν την ποσότητα του threading που θα επιτρέπουν. Το Slowloris πρέπει να περιμένει για να γίνει διαθέσιμες όλες οι υποδοχές (sockets), πριν να είναι επιτυχής στην κατανάλωσή τους, έτσι εάν μια ιστοσελίδα έχει υψηλή διαδικτυακή κυκλοφορία, μπορεί να πάρει λίγο χρόνο για τον ιστότοπο για να ελευθερώσετε υποδοχές (sockets) που διαθέτει. Σαν αποτέλεσμα είναι οι χρήστες να μην έχουν πρόσβαση στις υπηρεσίες ενός ιστοχώρου για αρκετές ώρες κάτι το οποίο μπορεί να επιφέρει καταστροφικά οικονομικά αποτελέσματα σε ένα οργανισμό ή μια επιχείρηση.

Στο σημείο αυτό θα παρουσιαστεί η εγκατάσταση του SlowLoris και η εντολή εκτέλεσης μιας επίθεσης άρνησης υπηρεσιών που θα χρησιμοποιηθεί και στις πειραματικές διαδικασίες που θα ακολουθήσουν. Αποθηκεύουμε τον πηγαίο κώδικα του SlowLoris ο οποίος είναι γραμμένος σε γλώσσα προγραμματισμού perl σε αρχείο της μορφής slowloris.pl. Μέσω της κονσόλας terminal του Kali Linux, εντοπίζουμε τον κατάλογο (directory) αποθήκευσης του πηγαίου κώδικα και στη συνέχεια εκτελούμε την παρακάτω εντολή : “perl slowloris.pl -dns 192.168.0.20” , όπου η διεύθυνση 192.168.0.20 είναι η διεύθυνση IP του εξυπηρετητή. Στις εικόνες που ακολουθούν εμφανίζεται η δημιουργία των sockets από το SlowLoris καθώς και η επιτυχής αποστολή πακέτο, με αποτέλεσμα να μην μπορεί ο διακομιστής να εξυπηρετήσει άλλους χρήστες που επιθυμούν να χρησιμοποιήσουν τις υπηρεσίες του. Στην Εικόνα 1 το SlowLoris συνδέεται μέσω της πόρτας 80 στον εξυπηρετητή και αποστέλλει πακέτα ανα 100 δευτερόλεπτα σε 1000 sockets.

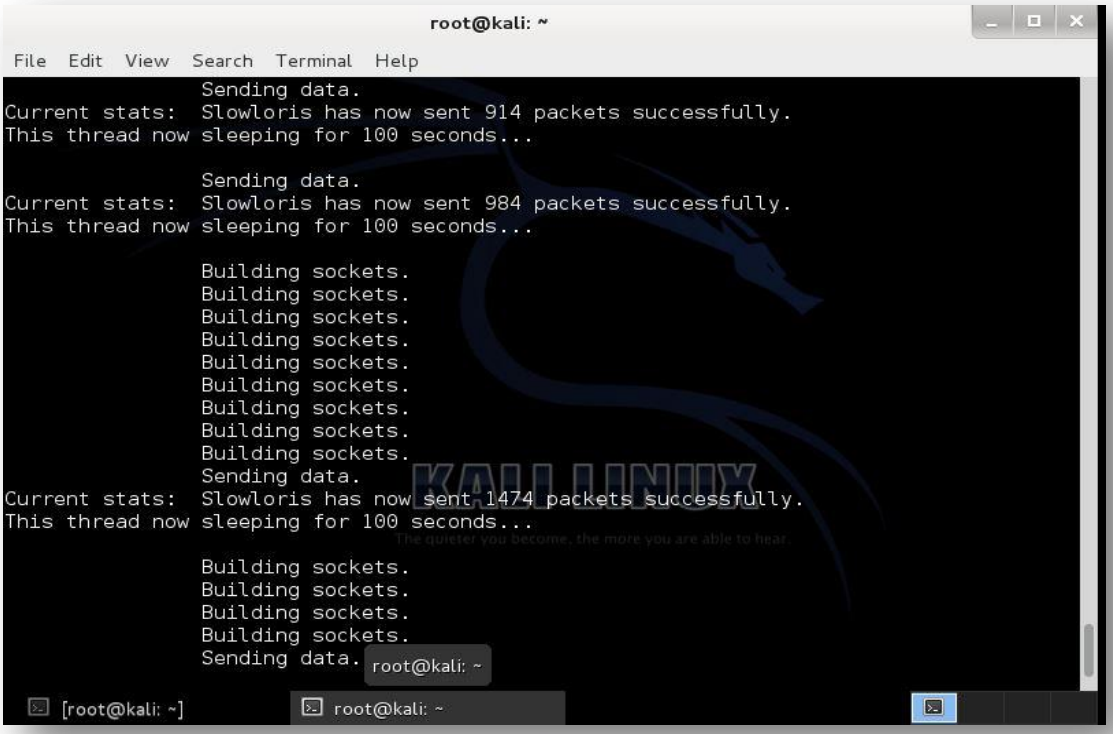
[26] Η διανομή Kali Linux διατίθεται στο παρακάτω σύνδεσμο : https://www.kali.org/

[27] Αρχεία πηγαίου κώδικα καθώς και πληροφορίες του SlowLoris: http://ha.ckers.org/slowloris/



Εικόνα 24. Δημιουργία sockets από το Slowloris.

Στην επόμενη εικόνα εμφανίζεται η συνεχής λειτουργία και αποστολή πακέτων ανά τακτά χρονικά διαστήματα από το SlowLoris , έτσι ώστε να μην προλαβαίνουν να ελευθερώνονται τα threads του διακομιστή. Το SlowLoris επιτρέπει την εκτέλεση και άλλων εντολών με περισσότερες παραμέτρους, για παράδειγμα αν είναι γνωστά τα χρονικά όρια ενός εξυπηρετητή αν δηλαδή ο εξυπηρετητής έχει ένα συγκεκριμένο χρονικό διάστημα και θέσουμε το χρονικό όριο σε όσο μικρότερη τιμή τότε θα καταναλωθούν γρήγορα οι διαθέσιμοι πόροι του συστήματος. Η εντολή "*perl slowloris.pl -dns 192.168.0.20 -timeout 2000 -num 500 -tcpto 5*" χρησιμοποιεί 500 sockets με χρονικό όριο στα 2.000 δευτερόλεπτα το οποίο αυξάνει το TCP όριο ανά 5 δευτερόλεπτα , οι περισσότεροι Apache διακομιστές τείνουν να έχουν λιγότερα από 400-600 sockets με μια προεπιλεγμένη ρύθμιση με αποτέλεσμα να εξαντλούνται πολύ γρήγορα οι διαθέσιμοι πόροι του συστήματος.

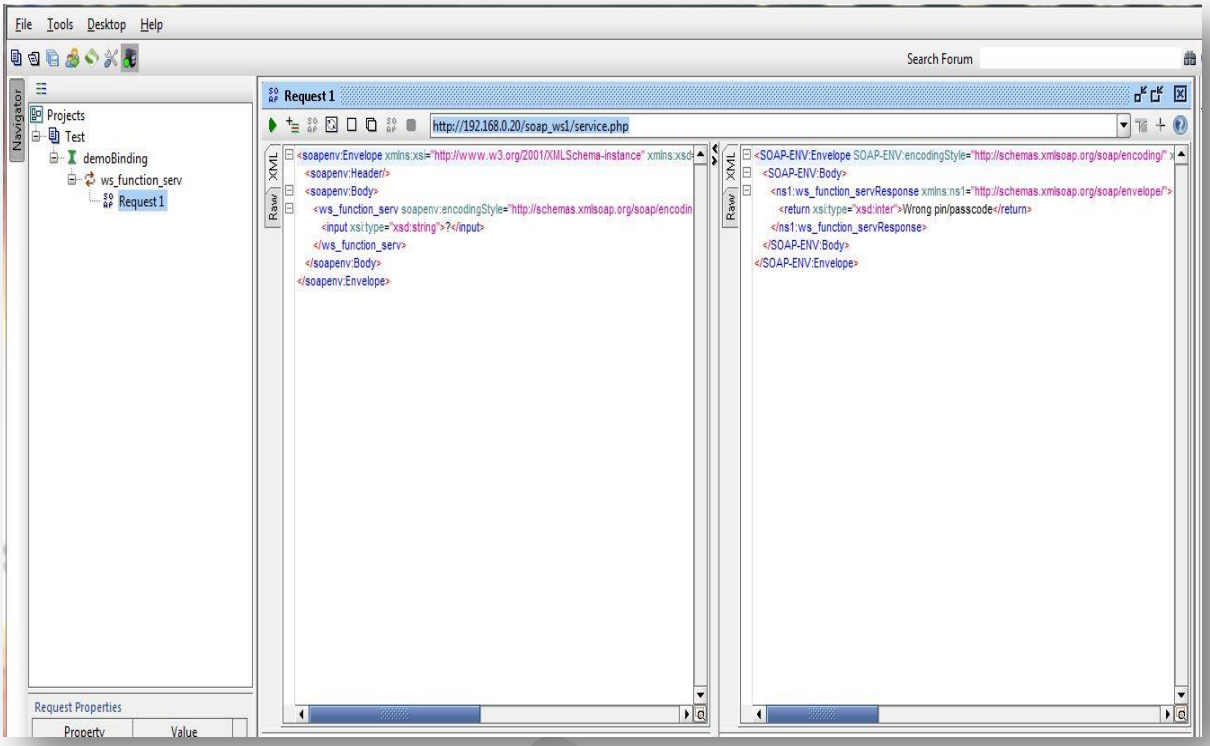


Εικόνα 25. Αποστολή πακέτων από το κλείσιμο των sockets.

Ένα ακόμη εργαλείο που θα παρουσιαστεί στα επόμενα παραδείγματα είναι το SoapUI[28]. Το SoapUI είναι μια εφαρμογή ανοιχτού κώδικα για δοκιμή διαδικτυακών υπηρεσιών για service-oriented αρχιτεκτονικές (SOA). Η λειτουργικότητα της εν λόγω εφαρμογής καλύπτει την επιθεώρηση υπηρεσιών ιστού, την κλήση των διαφόρων υπηρεσιών, την ανάπτυξη και την προσομοίωσα τους, δοκιμές και έλεγχο στη λειτουργία των υπηρεσιών ιστού. Σε ένα ενιαίο δοκιμαστικό περιβάλλον, το SoapUI παρέχει μια πληθώρα δοκιμών και υποστηρίζει όλα τα τυποποιημένα πρωτόκολλα και τεχνολογίες. Όπως θα παρουσιαστεί και στα επόμενα παραδείγματα γνωρίζοντας κάποιος το εξαγόμενο WSDL αρχείο μιας υπηρεσίας, με τη χρήση του SoapUI μπορεί να δημιουργήσει ένα WSDL σχέδιο και δίνοντας τις κατάλληλες παραμέτρους να του επιστραφούν διάφορα χρήσιμα αποτελέσματα από τις εκτελέσιμες υπηρεσίες ενός εξυπηρετητή. Στην παρακάτω εικόνα εμφανίζεται το περιβάλλον της εφαρμογής στο οποίο έχει δημιουργηθεί ένα δοκιμαστικό σχέδιο SOAP, στο παράδειγμα της εικόνας εκτελείται το WSDL το οποίο εξάγεται από ένα εξυπηρετητή με IP διεύθυνση: 192.168.0.20/soap_ws1/service.php?wsdl.

Κάτω και αριστερά από το παράθυρο “Request” εμφανίζεται το SOAP μήνυμα του πελάτη (client) σε XML μορφή και στα δεξιά η απάντηση του εξυπηρετητή της υπηρεσίας ιστού στο μήνυμα του πελάτη πάλι σε μορφή XML.

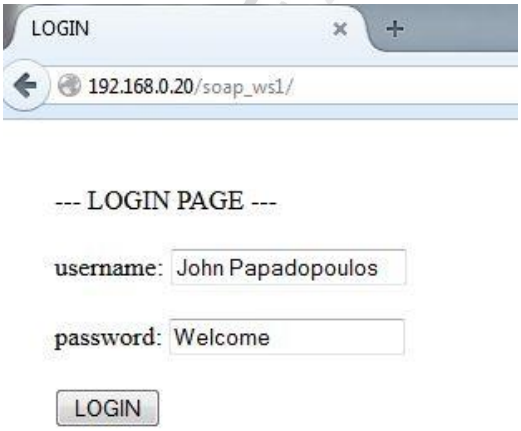
[28] Επίσημος ιστοχώρος για την εφαρμογή SoapUI : http://www.soapui.org/



Εικόνα 26. Περιβάλλον της εφαρμογής SoapUI.

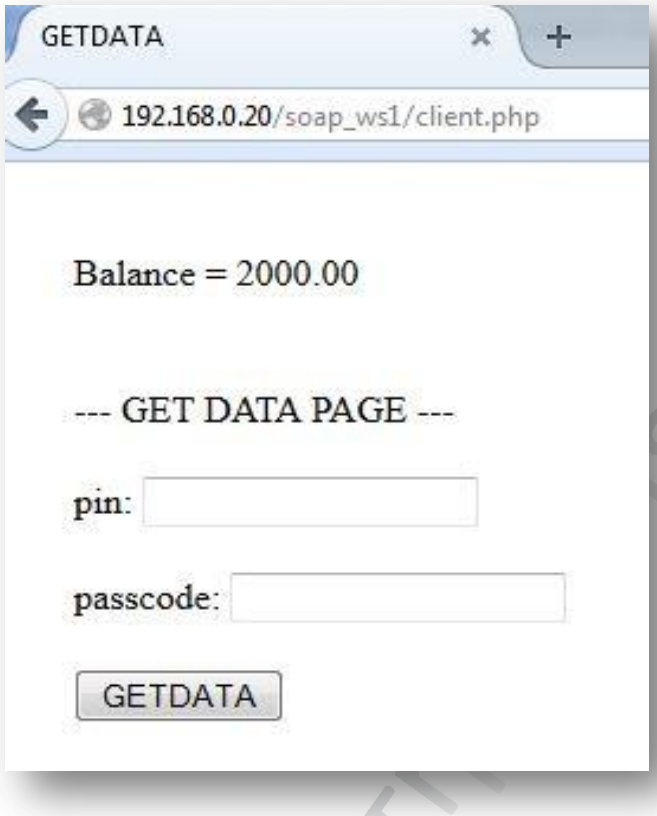
Στις ενότητες που ακολουθούν γίνεται η χρήση όλων των περιγραφέντων εργαλείων στα διάφορα πρακτικά σενάρια που θα παρουσιαστούν. Τέλος αξίζει να σημειωθεί ότι η ανάπτυξη του κώδικα και του παραδείγματος των υπηρεσιών ιστού έγινε με το πρόγραμμα Dreamweaver.

<u>Σενάριο 1ο</u> : Στην πρώτη πειραματική διαδικασία παρουσιάζεται μια απλή λειτουργία μιας υπηρεσίας ιστού μεταξύ των προγραμμάτων πελάτη και εξυπηρετητή. Η υπηρεσία περιέχει μια σελίδα εισόδου του χρήστη, στην οποία θα πρέπει να εισάγει ένα έγκυρο όνομα χρήστη και κωδικό. Στην περίπτωση που δεν εισαχθούν σωστά τα στοιχεία εμφανίζεται μήνυμα λάθους.



Εικόνα 27. Σελίδα εισαγωγής στην υπηρεσία. **Εικόνα28.Μήνυμα λάθους εισαγωγής στοιχείων.**

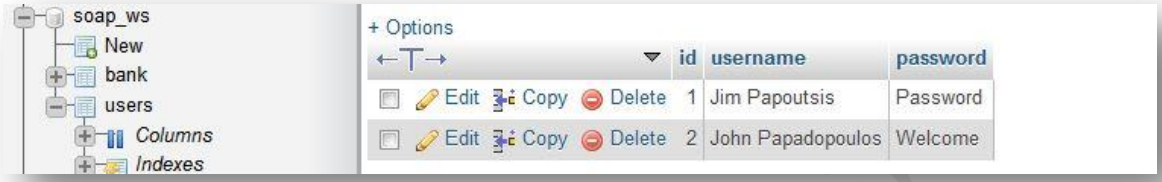
Στη συνέχεια ο χρήστης δρομολογείται στη σελίδα “Get Data” στην οποία συναντώνται δύο πεδία “pin” και “passcode”. Ο χρήστης συμπληρώνοντας σωστά τα δύο πεδία και πατώντας στο κουμπί “Get Data” του επιστρέφεται μέσω μιας υπηρεσίας ιστού το υπόλοιπο του λογαριασμού του. Στην περίπτωση που δεν εισαχθούν σωστά τα στοιχεία δεν επιστρέφεται υπόλοιπο.



Εικόνα 29. Επιστροφή υπολοίπου λογαριασμού.

Στο σημείο αυτό θα γίνει η επεξήγηση του κώδικα της υπηρεσίας ιστού που υλοποιήθηκε καθώς και η δημιουργία της βάσης έτσι ώστε να γίνουν περισσότερο κατανοητές οι λειτουργίες της εφαρμογής που παρουσιάζονται πειραματικά. Για πρακτικούς λόγους και για την διεξαγωγή της πειραματικής διαδικασίας έχει γίνει υλοποίηση μιας κοινής βάσης δεδομένων η οποία περιέχει ενδεικτικά στοιχεία χρηστών, τα οποία κρίνονται αρκετά για την επίτευξη των στόχων του πειράματος.

Στην αρχική σελίδα “index” γίνεται συναντώνται δύο πεδία “username” και “password” , με τα οποία ένας χρήστης δίνοντας τα σωστά δεδομένα μπορεί να εισαχθεί στην υπηρεσία. Τα πεδία “username” και “password” συνδέονται με την βάση δεδομένων “soap_ws” και συγκεκριμένα αντλεί δεδομένα από τον πίνακα “users”, όπως φαίνεται στην εικόνα που ακολουθεί.

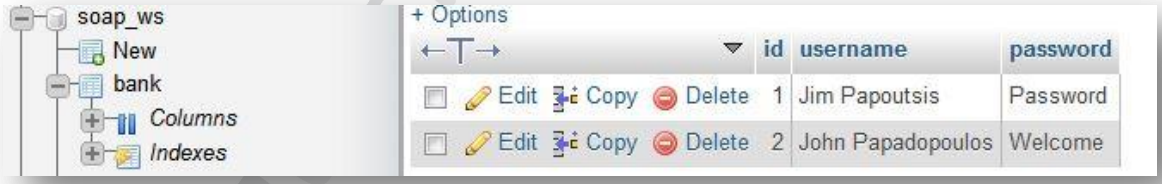


Εικόνα 30. Πίνακας “users” της βάσης δεδομένων “soap_ws”.

Στην αρχική σελίδα το γραφικό περιβάλλον (GUI) προστατεύεται από τα πεδία “username” και “password” και τα ερωτήματα προς τη βάση προστατεύονται από Sql Injection επίθεσης χρησιμοποιώντας την ready made συνάρτηση της PHP η οποία κάνει “sanitize” και λειτουργεί σαν φίλτρο στα δεδομένα που εισάγουν οι χρηστές σε μια υπηρεσία και τα ερωτήματα που κάνουν στη βάση του συστήματος αυτού:

```
$selCheck = "select * from users where username='".mysql_real_escape_string($_POST['username'])."' and password='".mysql_real_escape_string($_POST['password'])."'";
$runCheck = mysql_query($selCheck) or die(mysql_error());
```

Όταν ένας χρήστης εισαχθεί επιτυχώς στο σύστημα έχει πρόσβαση στην υπηρεσία της τράπεζας. Συμπληρώνοντας τα πεδία “pin” και “passcode” του επιστρέφεται το υπόλοιπο του λογαριασμού του. Τα πεδία “pin” και “passcode” περιέχονται στον πίνακα “bank” της βάσης δεδομένων “soap_ws” όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 31. Πίνακας “bank” της βάσης δεδομένων “soap_ws”.

Την αποστολή των δεδομένων “pin” και “passcode” την αναλαμβάνει ο πελάτης (client) της αποστέλλοντας ένα SOAP μήνυμα προς την διαδικτυακή υπηρεσία. Στον κώδικα που ακολουθεί δημιουργείται ένας νέος client:

```
        //εισαγωγή soap βιβλιοθήκης

        require 'lib/nusoap.php';

        //δημιουργία νέου client

$client = new nusoap_client("http://localhost/soap_ws1/service.php?wsdl");
```

Η παράμετρος $client είναι η μεταβλητή με τις SOAP λειτουργίες που περιλαμβάνονται στη βιβλιοθήκη NuSoap. Η πρώτη παράμετρος που δίνεται είναι η διεύθυνση του τελικού σημείου της υπηρεσίας ιστού. Ο client ζητάει το αρχείο WSDL από την υπηρεσία το οποίο δημιουργείται απευθείας. Στο επόμενο βήμα καλείται η υπηρεσία ιστού και εμφανίζονται τα αποτελέσματα με τη χρήση PHP κώδικα.

```
$params = array(
                    'pin' => $_POST['pin'],
                    'passcode' => $_POST['passcode'] );
          //καλείται η SERVICE ws function, αποστολή παραμέτρων,
          $balance = $client->call('ws_function_serv', $params);
//εμφάνιση αποτελεσμάτων
echo "Balance = ".$balance";
```

Αρχικά δημιουργείται ένας πίνακάς παραμέτρων που περιλαμβάνει “pin” και “passcode”. Στην επόμενη γραμμή η πρώτη παράμετρος αναφέρεται στη λειτουργία που καλείται (ws_function_serv), καθώς και η μεταβλητή $params που περιέχει την λίστα των παραμέτρων SOAP που έχουν δοθεί. Στο τέλος με την εντολή *echo* επιστρέφεται το υπόλοιπο που ζητήθηκε από την υπηρεσία.

Στα επόμενα βήματα περιγράφεται η δημιουργία του εξυπηρετητή που θα δέχεται τα SOAP μηνύματα. Στο μέρος του κώδικα που ακολουθεί, γίνεται η προσθήκη της βιβλιοθήκης NuSoap, στη συνέχεια δημιουργείται η μεταβλητή *$server* η οποία περιέχει όλες τις SOAP λειτουργίες. Η τρίτη γραμμή κώδικα περιγράφει στον διακομιστη NuSoap για το ποια έκδοση του WSDL θα υποστηρίζεται. Η τελευταία γραμμή κώδικα καταγράφει μια νέα λειτουργία SOAP στην ίδια την υπηρεσία ιστού.

```
require 'lib/nusoap.php';

$server = new nusoap_server(); // δημιουργία instance εξυπηρετητή

$server->configureWSDL('demo',"urn:demo");
//υποστήριξη εξυπηρετητή

$server->register("ws_function_serv"); //καταγραφή νέας λειτουργίας
```

Στο επόμενο κομμάτι κώδικα εμφανίζεται η κυρίως λειτουργία της υπηρεσίας. Η λειτουργία περιέχει την εφαρμογή της υπηρεσίας ιστού και λαμβάνει τις εισόδους SOAP απευθείας ως παραμέτρους.

```
function ws_function_serv($pin,$passcode){

        //παίρνει τα δεδομένα των χρηστών  από την βάση δεδομένων  βάση των δεδομένων εισόδου που δόθηκαν

        $sql = "select * from bank where pin='".$pin."' and passcode='".$passcode."'";

        $run =  mysql_query($sql) or die(mysql_error());

        if(mysql_num_rows($run)>0){

                $row = mysql_fetch_assoc($run);

                $balance = $row['balance']; //επιστρέφει το υπόλοιπο του χρήστη

        } else {

                $balance = "Wrong pin/passcode"; // κανένα αρχείο με τα δεδομένα εισόδου του χρήστη

        }

        return $balance; //επιστροφή της τιμής σαν SOAP μήνυμα

}
```

Στο τελευταίο κομμάτι του κώδικα περιγράφεται η εκτέλεση της υπηρεσίας ιστού, κατά την οποία δημιουργείται ένας HTTP ακροατής (listener) ο οποίος καλεί την υπηρεσία.

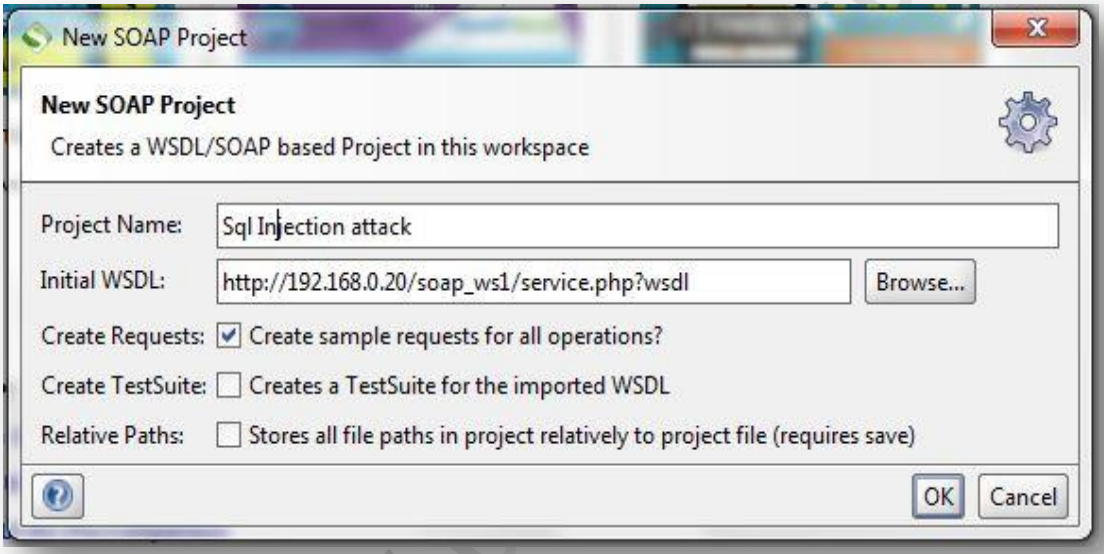
```
// δημιουργία HTTP ακροατή (listener)

$HTTP_RAW_POST_DATA =
isset($HTTP_RAW_POST_DATA) ?
$HTTP_RAW_POST_DATA : '';

$server ->service($HTTP_RAW_POST_DATA);
```

Το *$HTTP_RAW_POST_DATA* θα πρέπει να περιέχει την SOAP XML αίτηση. Η μεταβλητή *$server ->service* αναλύει το XML αρχείο, καλεί τη συνάρτηση και δημιουργεί την απάντηση πάλι σε XML μορφή. Η πραγματική διαδικτυακή υπηρεσία έχει ήδη κληθεί μέσω του πρωτοκόλλου HTTP για να πάρει την τρέχουσα σελίδα.

Τα στοιχεία του κάθε χρήστη είναι μοναδικά. Στο σημείο αυτό, όπως θα φανεί και από τα εργαλεία ψηφιακών επιθέσεων που περιγράφτηκαν στις προηγούμενες ενότητες και τα αποτελέσματα τους, η υπηρεσία προστατεύεται από το γραφικό περιβάλλον με την ύπαρξη των πεδίων “pin” και “passcode”, δηλαδή αν ένας χρήστης δώσει λανθασμένα στοιχεία δεν θα πάρει κάποιο υπόλοιπου λογαριασμού, αλλά δεν προστατεύεται από επιθέσεις τύπου Sql Injection όπως θα δούμε με την χρήση του εργαλείου SoapUI ένας κακόβουλος χρήστης μπορεί να πάρει αποτελέσματα από την υπηρεσία ιστού δίνοντας μια παράμετρο προς την βάση η οποία είναι αληθής (1' or '1' = '1).

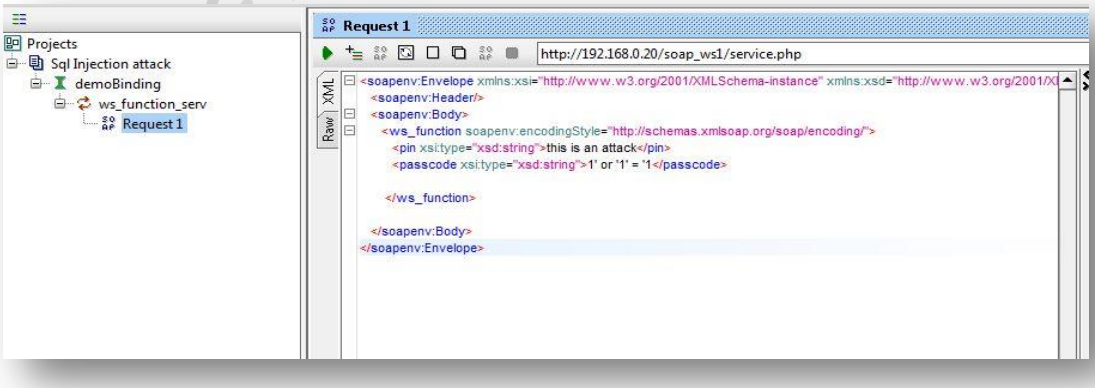
Εκτός από τις επιθέσεις Sql Injection, η υπηρεσία είναι ευάλωτη και σε επιθέσεις άρνησης υπηρεσιών (DoS attacks), κάτι που καθιστά αδύνατο για ένα διακομιστή να εξυπηρετήσει άλλες αιτήσεις. Σε κάθε περίπτωση θα αποδειχθεί ότι τα δεδομένα που μπορούν να συλλεχθούν από τέτοιο είδους επιθέσεις δεν είναι αρκετά.

Επίθεση Sql Injection : Στην παρούσα παράγραφο θα γίνει η χρήση του εργαλείου SoapUI που παρουσιάστηκε στις προηγούμενες ενότητες. Υποθέτουμε ότι ένας κακόβουλος χρήστης γνωρίζει το παραγόμενο WSDL αρχείο της διαδικτυακής υπηρεσίας. Δημιουργώντας ένα νέο σχέδιο επίθεσης μέσω της εφαρμογής δίνει αρχικά την διεύθυνση του WSDL αρχείου.



Εικόνα 32. Δημιουργία ενός νέου σχεδίου SOAP.

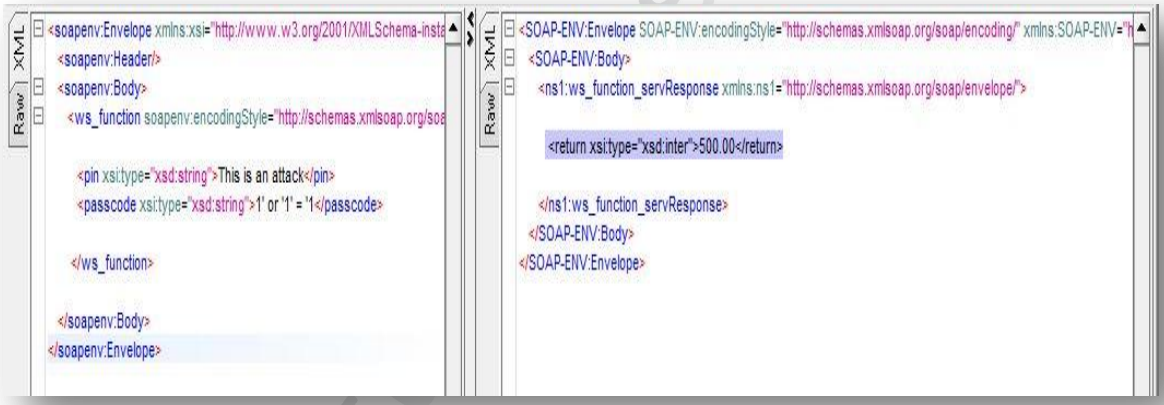
Στην επόμενη εικόνα, στην αριστερή στήλη παρουσιάζεται το σχέδιο μιας Sql Injection επίθεσης. Στην δεξιά στήλη εμφανίζεται το ερώτημα που θα αποσταλεί στην υπηρεσία σε XML μορφή.



Εικόνα 33. SoapUI σχέδιο.

Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα πεδία “pin” και “passcode” που εμφανίζονται στο SOAP μήνυμα. Όπως παρατηρείται εμφανίζεται η λειτουργία ws_function μαζί με τα πεδία pin” και “passcode”. Ο κακόβουλος χρήστης δίνοντας τις κατάλληλες τιμές έχει την δυνατότητα να εκμεταλλευτεί την ευπάθεια στην βάση SQL και να του επιστραφεί ένα αποτέλεσμα. Όπως φαίνεται και στο παράδειγμα που ακολουθεί ο χρήστης δίνει μια αληθή τιμή η οποία συνηθίζεται να χρησιμοποιείται σε επιθέσεις Sql Injection, “1' or '1' = '1” και του επιστρέφεται απάντηση μαζί με το υπόλοιπο ενός λογαριασμού.

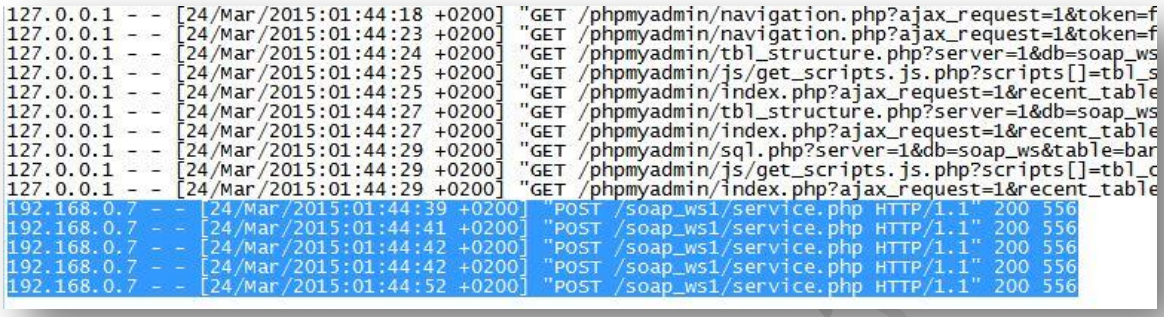
```
<ws_function
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/enc
oding/">

<pin xsi:type="xsd:string">This is an attack</pin>
<passcode xsi:type="xsd:string">1' or '1' = '1</passcode>

   </ws_function>
```



Εικόνα 34. Επιστροφή αποτελέσματος υπολοίπου λογαριαμού από την εφαρμογή SoapUI.

Όπως φαίνεται στην εικόνα Εικόνα 34, ο χρήστης δίνοντας σαν παραμέτρους pin = “This is an attack” και passcode = “1' or '1' = '1”, του επιστρέφεται το υπόλοιπο – balance =500.

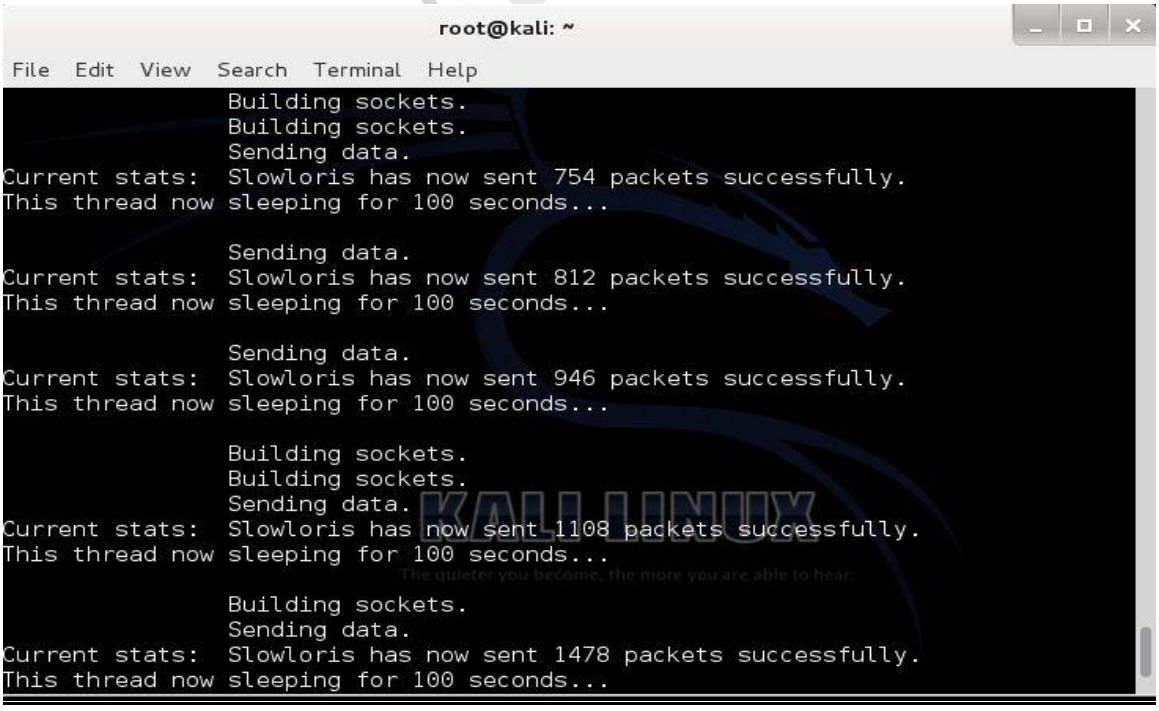
Στην περίπτωση που ένας ειδικός ερευνητής θα επιθυμούσε να συλλέξει πειστήρια για μια τέτοιου είδους επίθεση στη συγκεκριμένη υπηρεσία ιστού αυτό θα ήταν αδύνατο καθώς δεν είναι δυνατό να καταγραφεί η κακόβουλη ψηφιακή επίθεση από κανένα εργαλείο της υπηρεσίας ιστού. Εξετάζοντας το αρχείο καταγραφής του Apache διακομιστή εμφανίζονται μόνο νόμιμες κινήσεις στην υπηρεσία, με αποτέλεσμα να μην μπορούν να εντοπιστούν οι υπεύθυνοι της επίθεσης και να μην γίνονται αντιληπτές οι ευπάθεια της υπηρεσίας.



Εικόνα 35. Αρχείο καταγραφής Apache.

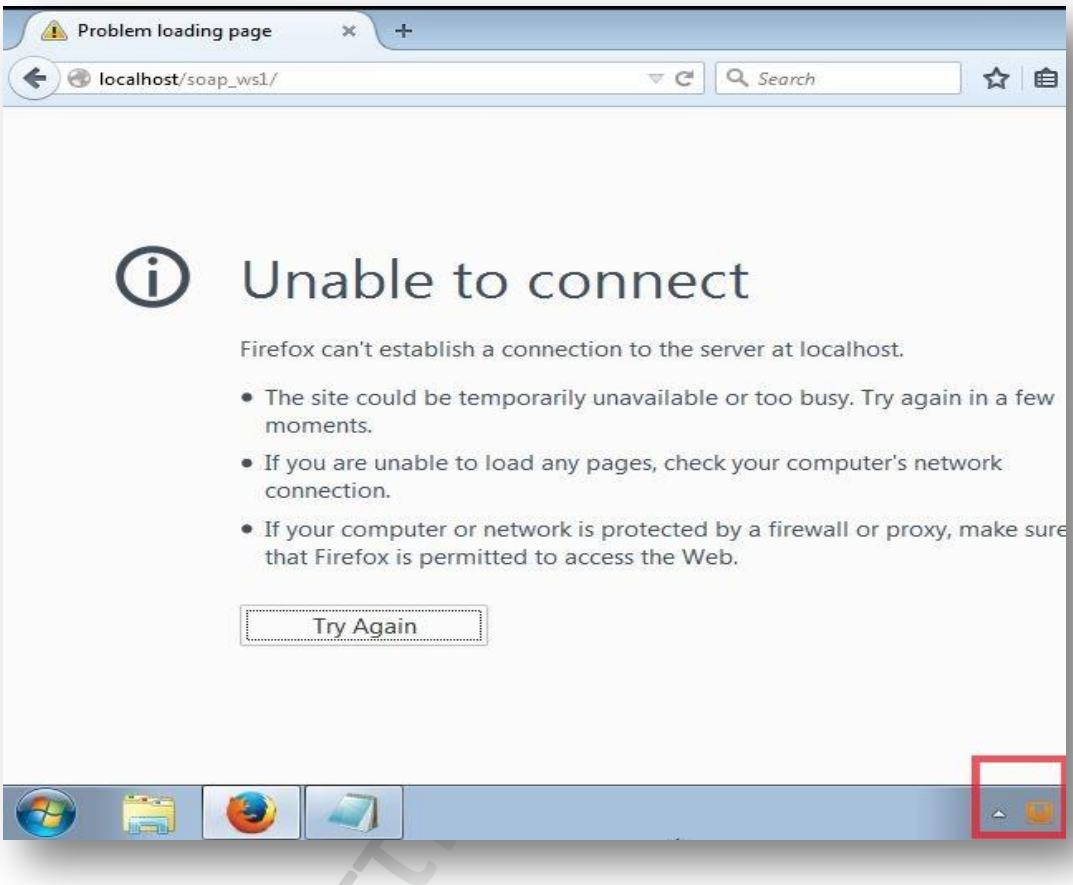
Επίθεση άρνησης υπηρεσιών: Στο συγκεκριμένο παράδειγμα θα γίνει επίθεση στην περιγραφείσα υπηρεσία με το εργαλείο SlowLoris. Μετά την χρήση του εργαλείου ο διακομιστής δεν θα έχει την δυνατότητα να εξυπηρετήσει άλλα αιτήματα και θα πέσει σε κατάσταση αδράνειας. Μετά την διεξαγωγή του πειράματος θα γίνει εύκολα αντιληπτό ότι δεν υπάρχουν τα αντίμετρα εκείνα τα οποία θα μπορέσουν να αποτρέψουν μια επίθεση άρνησης υπηρεσιών (DoS) ή ακόμα να συλλεχθούν όλα τα απαραίτητα δεδομένα τα οποία θα υπεδείκνυαν σε μια εγκληματολογική έρευνα τους υπαίτιους μιας επίθεσης.

Εκτελώντας την εντολή "*perl slowloris.pl –dns 192.168.0.20*", όπου η διεύθυνση 192.168.0.20 είναι η IP διεύθυνση της υπηρεσίας, το SlowLoris αποστέλλει μέσω τις πόρτας 80 μεγάλο αριθμό πακέτων ανα τακτά χρονικά διαστήματα με αποτέλεσμα να καθίσταται αδύνατο να ελευθερωθούν sockets στον διακομιστή.



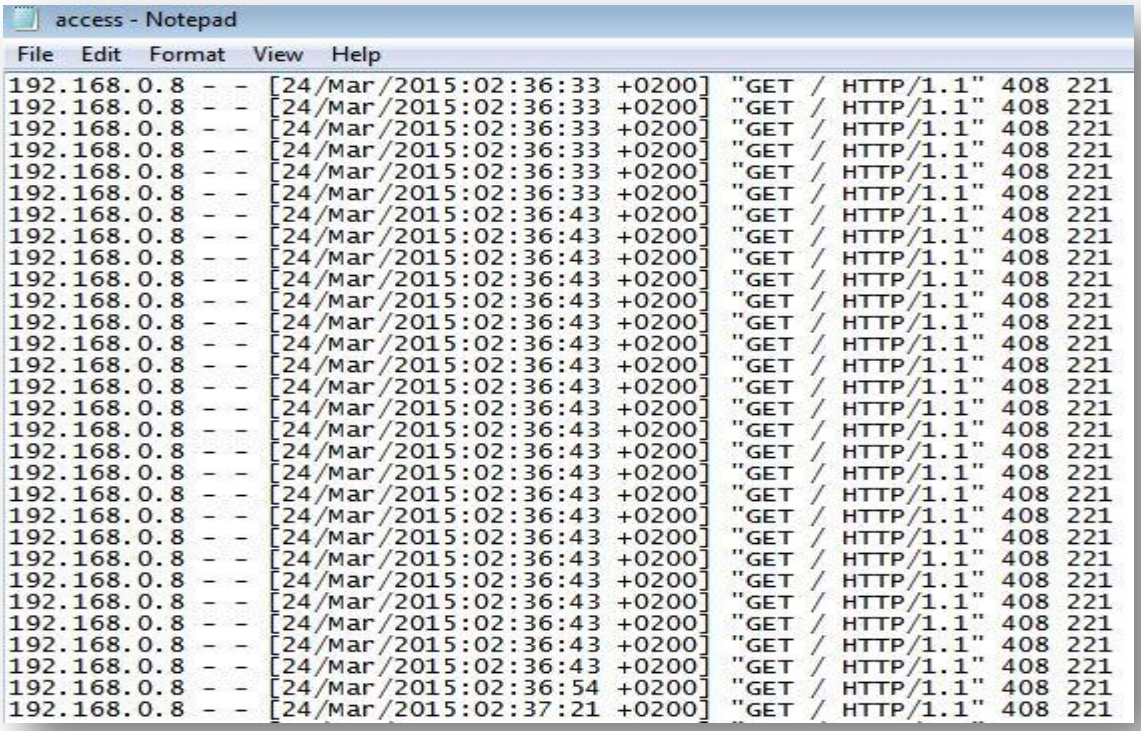
Εικόνα 36.Αποστολή πακέτων με το εργαλείο SlowLoris.

Στην επόμενη εικόνα παρατηρούμε ότι η υπηρεσία δεν είναι διαθέσιμη και ο εξυπηρετητής Apache δεν μπορεί να εκκινήσει (εικονίδιο στο κόκκινο πλαίσιο) όσο αποστέλλουμε πακέτα με το SlowLoris.



Εικόνα 37. Μη διαθέσιμη υπηρεσία ιστού.

Εάν ένας ερευνητής της Δικανικής πληροφορικής επιθυμούσε να συλλέξει μερικά δεδομένα που θα αποτελούσαν αποδεικτικά στοιχεία της ψηφιακής επίθεσης, η έρευνα θα αποδεικνυόταν άκαρπη καθώς το μόνο αποδεικτό στοιχείο θα ήταν το αρχείο καταγραφής του Apache διακομιστή στο οποίο , μετά το συμβάν της επίθεσης DoS ,θα παρατηρούσε απλώς πολλά αιτήματα από μια διεύθυνση IP τα οποία δεν θα μπορούσαν να αποδείξουν ότι αποτελούν ένα συμβάν επίθεσης ή απλά μια είσοδο στην υπηρεσία.



Εικόνα 38.Αρχείο καταγραφής Apache μετά από επίθεση άρνησης υπηρεσιών.

Συμπεραίνεται λοιπόν ότι σε μια περίπτωση σενάριο όπως το πρώτο σενάριο, οι υπηρεσίες παραμένουν απροστάτευτες από κάθε είδους ψηφιακή επίθεση, δεν υπάρχουν τα αντίμετρα ή οι αυτοματισμοί που θα μπορούσαν να καταγράψουν, να εμποδίσουν ή να ειδοποιήσουν για ένα συμβάν επίθεσης. Το έργο ενός Δικανικού ερευνητή θα ήταν αρκετά δύσκολο σε μια τέτοια περίπτωση καθώς δεν θα μπορούσε να αντλήσει τα απαραίτητα δεδομένα τα οποία θα συντελούσαν στην διερεύνηση της επίθεσης.

Σενάριο 2^{ο} : Στο δεύτερο κατά σειρά σενάριο θα γίνει προσπάθεια να καλυφθούν οι ευπάθειες της υπηρεσίας που περιγράφτηκαν στο πρώτο σενάριο και να αντιμετωπιστούν αποτελεσματικά οι επιθέσεις Sql Injection και άρνησης υπηρεσιών (DoS). Επίσης θα εξηγηθούν αναλυτικά οι αλλαγές στο τεχνολογικό περιβάλλον σε σχέση με τις υποθέσεις και τις υλοποιήσεις του 1^{ου} σεναρίου.

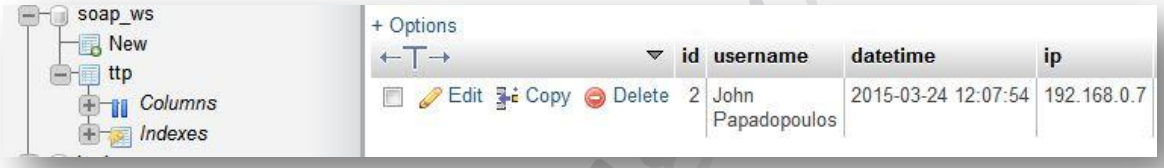
Ένα από τα κυριότερα εργαλεία που θα παρουσιαστεί είναι αυτό της τρίτης έμπιστης οντότητας (Trusted Third Party) ή διαφορετικά TTP. Ο TTP είναι ένα διακομιστής ο οποίος έχει το ρόλο του «μεσάζοντα» μεταξύ του πελάτη και του διακομιστή. Ο TTP διακομιστής αναλαμβάνει να μεταβιβάσει το SOAP μήνυμα από τον πελάτη (client) στην υπηρεσία του εξυπηρετητή, στη συνέχεια η απάντηση του τελικού σημείου (end point) της υπηρεσίας ιστού επιστρέφεται πάλι στο TTP διακομιστή και αυτός αναλαμβάνει μέσω SOAP μηνύματος να στείλει τα τελικά αποτελέσματα στον χρήστη.

Ο TTP εξυπηρετητής παρουσιάζει και μια ακόμα λειτουργία αυτή της εποπτείας των συναλλαγών μεταξύ του πελάτη και της υπηρεσίας του τελικού εξυπηρετητή. Ο TTP καταγράφει σε μια βάση δεδομένων ώρα που ξεκίνησε ένα αίτημα από τον πελάτη, ένα μοναδικό αριθμό id, την διεύθυνση

IP του χρήστη, καθώς επίσης και το όνομα χρήστη “username”, όπως εμφανίζεται στο μέρος του κώδικα που ακολουθεί.

```
//εισαγωγή αρχείου καταγραφής στην βάση δεδομένων

        $sql = "insert into ttp (username, datetime, ip) values
('".$username."','".$wsCallDatetime."','".$ip."')";

        $run = mysql_query($sql) or die(mysql_error());
```

Στην επόμενη εικόνα εμφανίζεται η δομή και τα πεδία του πίνακα ttp της βάσης soap_ws.



Εικόνα 39. Πίνακας του Trusted third Party (TTP) της βάσης δεομένων soap_ws.

Στη τρέχουσα παράγραφο θα παρουσιαστεί η λειτουργία και η δημιουργία του TTP διακομιστή και πώς αυτός συνεργάζεται με τις υπηρεσίες πελάτη και τελικού εξυπηρετητή. Όπως περιγράφηκε στο 1^{ο} σενάριο έτσι και σε συγκεκριμένο παράδειγμα, δημιουργείται μια καινούργια μεταβλητή *$client* η οποία αυτή τη φορά απευθύνεται στο WSDL αρχείο της υπηρεσίας που βρίσκεται στο TTP. Στη συνέχεια δημιουργείται ο πίνακας παραμέτρων που θα αποσταλεί στην υπηρεσία του TTP και η μεταβλητή *$client* καλεί τη λειτουργία (function) του TTP “*ws_function_ttp*” δίνοντας τις απαραίτητες παραμέτρους $params.

```
//δημιουργία νέου client για το ws του ttp

        $client = new nusoap_client("http://192.168.0.15/soap_ws2/ttp.php?wsdl");

//παράμετροι εισόδου από τον χρήστη και καταγραφή του username, IP διεύθυνση

        $params = array(

                'pin' => mysql_real_escape_string($_POST['pin']), // sanitize pin

                'passcode' => mysql_real_escape_string($_POST['passcode']), // sanitize
passcode

                'username' => $_SESSION['username'],

                'ip' => $_SERVER['REMOTE_ADDR']   );

        $balance = $client->call('ws_function_ttp', $params); ////καλείται η ttp ws function,
αποστολή παραμέτρων
```

Στο παραπάνω κώδικα παρατηρούμε ότι γίνεται χρήση της εντολής “mysql_real_escape”, έτσι ώστε να αποφευχθούν οι επιθέσεις Sql Injection όταν κάποιος χρήστης εισάγει τιμές στα πεδία “pin” και “passcode”. Επιπροσθέτως δίνονται σαν παράμετροι και καταγράφονται το όνομα χρήστη “username” και η IP διεύθυνση του χρήστη που κάνει το αίτημα την δεδομένη χρονική στιγμή.

Εστιάζοντας στο μέρος του διακομιστή της τρίτης έμπιστης οντότητας – TTPκαι στο κομμάτι του κώδικα που ακολουθεί, αρχικά γίνεται η προσθήκη της βιβλιοθήκης NuSoap, στη συνέχεια δημιουργείται η μεταβλητή *$server* που αφορά τη δημιουργία του TTP εξυπηρετητή η οποία περιέχει όλες τις απαραίτητες SOAP λειτουργίες. Η επόμενη γραμμή κώδικα περιγράφει στον για την έκδοση του WSDL που θα υποστηρίζεται. Η τελευταία γραμμή κώδικα καταγράφει μια νέα λειτουργία SOAP στην ίδια την υπηρεσία ιστού.

```
require 'lib/nusoap.php';

$server = new nusoap_server(); // δημιουργία instance εξυπηρετητή

$server->configureWSDL('demo',"urn:demo");
//υποστήριξη εξυπηρετητή

$server->register("ws_function_ttp"); //καταγραφή νέας λειτουργίας
```

Στη συνέχεια δημιουργείται, όπως παρουσιάστηκε και στο πρώτο σενάριο , ο HTTP ακροατής (HTTP listener), ο οποίος αναλαμβάνει να καλέσει την υπηρεσία ιστού.

```
// δημιουργία HTTP ακροατή (listener)

$HTTP_RAW_POST_DATA =
isset($HTTP_RAW_POST_DATA) ?
$HTTP_RAW_POST_DATA : '';

$server ->service($HTTP_RAW_POST_DATA);
```

Ο TTP διακομιστής αναλαμβάνει να προωθήσει τα SOAP μηνύματα που λαμβάνει από τον πελάτη προς τη τελική υπηρεσία, στο συγκεκριμένο παράδειγμα η τελική ονομασία αναφέρεται σαν “service_ws”. Για να επιτευχθεί αυτή η αποστολή των δεδομένων δημιουργείται και καθορίζεται μια νέα υπηρεσία ιστού που θα στέλνει τα αιτήματα από το TTP διακομιστή σε αυτόν της τελικής υπηρεσίας. Όλα τα παραπάνω επιτυγχάνονται εκτελώντας τον παρακάτω κώδικα.

```
//δημιουργία soap client με τη service_ws

        $client = new
nusoap_client("http://192.168.0.20/soap_ws2/service.php?wsdl");
//προσδιορισμός  soap client
```

Στη συνέχεια της λειτουργίας του TTP γίνεται ο προσδιορισμός των παραμέτρων που θα αποσταλούν στο "*service_ws*" και η κλήση της υπηρεσίας ιστού "*ws_function_serv*", μαζί με τις παραμέτρους "pin" και "passcode".

```
$params = array(
                    'pin' => $_POST['pin'],
                    'passcode' => $_POST['passcode'] );
          //καλείται η SERVICE ws function, αποστολή παραμέτρων,
          $balance = $client->call('ws_function_serv', $params);
//εμφάνιση αποτελεσμάτων
return $balance; //επιστροφή υπολοίπου στο client
```

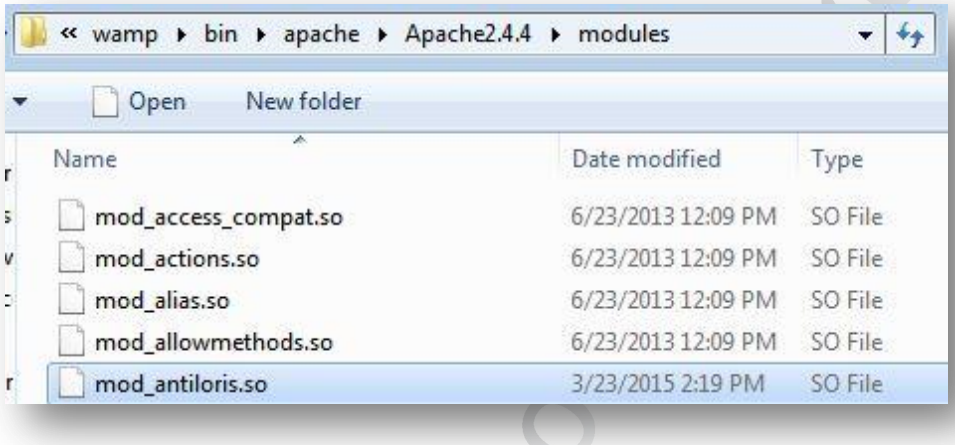
Στο τελευταίο μέρος της λειτουργίας του, ο TPP διακομιστής αναλαμβάνει να αποθηκεύσει τα αρχεία καταγραφής (log files) στη βάση δεδομένων του. Γίνεται καταγραφή της ώρας και της ημερομηνίας που στάλθηκε το SOAP μήνυμα καθώς επίσης του ονόματος χρήστη (username) και της διεύθυνσης IP του χρήστη.

```
//εισαγωγή αρχείων καταγραφής στη βάση δεδομένων
          $sql = "insert into ttp (username, datetime, ip) values
('".$username."','".$wsCallDatetime."','".$ip."')";
          $run = mysql_query($sql) or die(mysql_error());
```

Τέλος, η υπηρεσία "*service_ws*" αναλαμβάνει να αναζητήσει στη βάση δεδομένων και να επιστρέψει τα αποτελέσματα στο TTP που του ζητήθηκαν. Ο TTP με την σειρά αναλαμβάνει να τα δρομολογήσει προς την υπηρεσία του client, όπου και εμφανίζονται στο χρήστη με τη χρήση της εντολής "*echo $balance*".

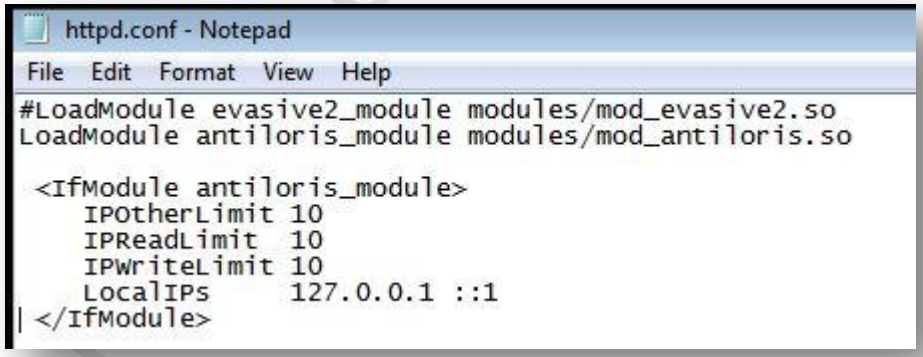
```
function ws_function_serv($pin,$passcode){
          sql = "select * from bank where pin='".$pin."' and
passcode='".$passcode."'";
          $run =  mysql_query($sql) or die(mysql_error());
if(mysql_num_rows($run)>0){
                    $row = mysql_fetch_assoc($run);
                    $balance = $row['balance'];
} else {  $balance = "Wrong pin/passcode";
}         return $balance;  }
```

Ένα ακόμα εργαλείο που θα χρησιμοποιηθεί σαν αντίμετρο κατά των επιθέσεών άρνησης υπηρεσιών DoS είναι το mod_antiloris. Το mod_antiloris, όπως έχει αναφερθεί και σε προηγούμενες ενότητες είναι πρόσθετο εργαλείο που μπορεί να εγκατασταθεί στη λειτουργία του Apache εξυπηρετητή. Το mod_antiloris είναι ικανό να αποτρέψει επιθέσεις άρνησης υπηρεσιών ενάντια σε ένα Apache εξυπηρετητή. Το mod_antiloris μέσω ενός σετ κανόνων μπορεί να περιορίσει τον αριθμό των νημάτων (threads) όταν ένας εξυπηρετητής βρίσκεται σε κατάσταση ανάγνωσης (Read state). Η εγκατάσταση του mod_antiloris γίνεται με την αποθήκευση ενός μεταγλωτισμένου αρχείου .c σε μορφή .so στο φάκελο modules του Apache του εργαλείου WampServer.



Εικόνα 40. Αποθήκευση του mod_antiloris.so μεταγλωττισμένου αρχείου.

Στη συνέχεια θα πρέπει να φορτωθεί και να ενεργοποιηθεί το εργαλείο mod_antiloris στο httpd.conf αρχείο του Apache εξυπηρετητή όπως εμφανίζεται στην παρακάτω εικόνα. Για να ενεργοποιηθεί ένα module δεν πρέπει να προηγείται ο χαρακτήρας “#” πριν από αυτό.



Εικόνα 41. Φόρτωση mod_antiloris στο httpd.conf αρχείο του Apache εξυπηρετητή.

Στην Εικόνα 41παρουσιάζονται οι βασικοί κανόνες οι οποίοι είναι ικανοί να αποτρέψουν μια επίθεση άρνησης υπηρεσιών. Η εισαγωγή των κανόνων εκκινεί με τη χρήση της εντολής

"<*IfModule ….*>" και κλείνει με τη χρήση "</*IfModule ….*>" . Οι κανόνες που εμφανίζονται κάτω από την εντολή "<*IfModule ….*> έχουν τις εξής λειτουργίες:

- Η IPOtherLimit λειτουργία, προσδιορίζει μέγιστο αριθμό ταυτόχρονων αδρανών συνδέσεων για κάθε IP διεύθυνση.
- Η IPReadLimit λειτουργία, ελέγχει το μέγιστο αριθμό ταυτόχρονων συνδέσεων σε κατάσταση ανάγνωσης για κάθε IP διεύθυνση.
- Η IPWriteLimit λειτουργία, ελέγχει το μέγιστο αριθμό ταυτόχρονων συνδέσεων σε κατάσταση εγγραφής για κάθε IP διεύθυνση.
- Η LocalIPs λειτουργία, προσδιορίζει τη λίστα των IP διευθύνσεων των οποίων οι συνδέσεις επιτρέπονται πάντα.

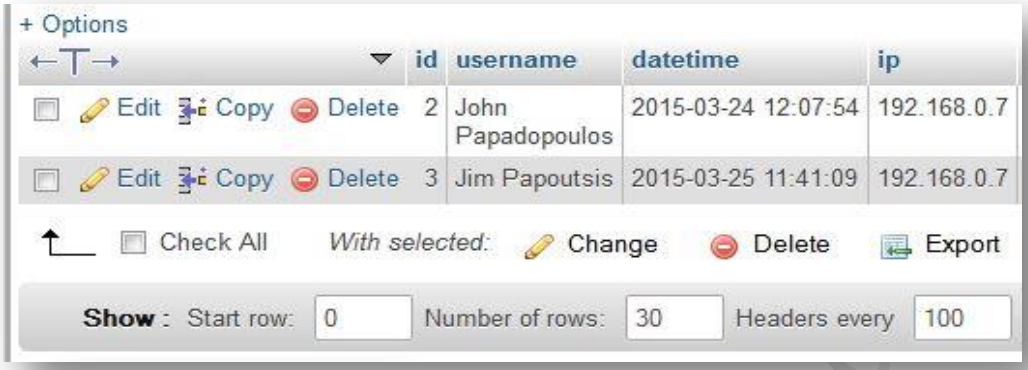
Συνοψίζοντας το παράδειγμα της εικόνας το οποίο θα εφαρμοστεί και στο πειραματικό μέρος θα επιτρέψει το άνοιγμα δέκα συνδέσεων σε κάθε κατάσταση από το σύνολο των τριάντα συνδέσεων και θα επιβάλει όρια στις συνδέσεις του localhost (127.0.0.1).

Όπως και στο πρώτο σενάριο το πειραματικό τεχνολογικό περιβάλλον παρουσιάζει ευπάθεια σε επιθέσεις τύπου Sql Injection και παρουσιάζει αδυναμία στο να αντιμετωπίσει επιθέσεις άρνησης υπηρεσιών (DoS attacks). Σοβαρό μειονέκτημα είναι ότι δεν παρέχονται όλες αυτές οι πληροφορίες οι οποίες θα υποδείκνυαν ότι το πληροφοριακό σύστημα έχει υποστεί επίθεση με αποτέλεσμα μια Δικανική εγκληματολογική έρευνα να μην είναι σε θέση να υποδείξει τους υπαίτιους μιας ηλεκτρονικής επίθεσης στις υπηρεσίες ιστού του οργανισμού. Στα παραδείγματα επιθέσεων που ακλουθούν θα εξάγουμε συμπεράσματα αν οι αυτοματισμοί και τα εργαλεία του TTP και του mod_antiloris τα οποία που περιγράφτηκαν ανωτέρω, είναι ικανά να προστατέψουν τις υπηρεσίες ιστού και να προσφέρουν όλη αυτή τη πληροφόρηση που απαιτείται από μια Δικανική έρευνα έτσι ώστε να ανακατασκευαστεί το συμβάν της επίθεσης και να εντοπιστούν οι υπαίτιοι της.

Στο εικονικό περιβάλλον που έχει σχεδιαστεί ο TTP διακομιστής και οι υπηρεσίες βρίσκεται στη διεύθυνσή IP: 192.168.0.15 και η τελική υπηρεσία ιστού service_ws στην διεύθυνση IP : 192.168.0.20.

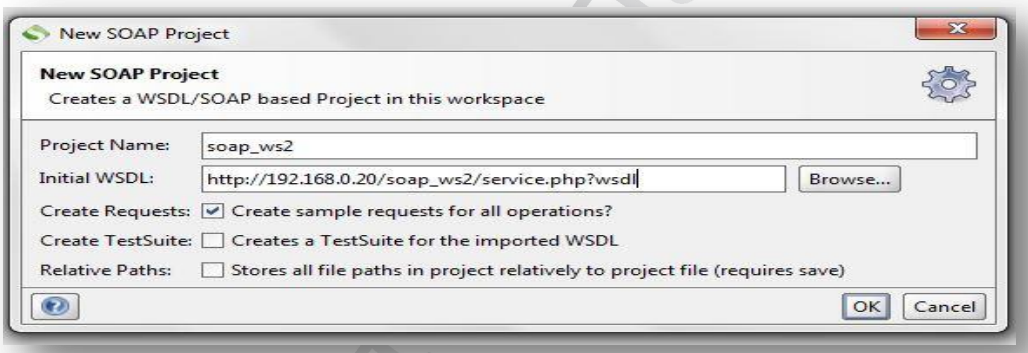
Επίθεση Sql Injection : Με τη χρήση του εργαλείου SoapUI όπως παρουσιάστηκε και στο πρώτο πειραματικό σενάριο, θα εξεταστεί αν όλα τα αντίμετρα και οι αυτματισμοί που εφαρμόστηκαν είναι ικανά να ελέγξουν και κατ' επέκταση να αποτρέψουν μια επίθεση Sql Injection στη βάση δεδομένων της υπηρεσίας.

Σε πραγματικές συνθήκες εάν ένας χρήστης εισαχτεί στο σύστημα με νόμιμο τρόπο και ζητήσει από την υπηρεσία να του επιστραφεί το υπόλοιπο του λογαριασμού του τότε το αρχείο καταγραφής του TTP διακομιστή θα πρέπει να έχει την ακόλουθη εικόνα στην οποία εμφανίζονται η ώρα εισόδου, το όνομα χρήστη και το id του, καθώς και η διεύθυνση IP του χρήστη. Συμπεραίνουμε ότι σε μια τέτοια περίπτωση ο TTP διακομιστής λειτουργεί με σωστό τρόπο στην καταγραφή των στοιχείων που αφορά τη συναλλαγή μεταξύ πελάτη και εξυπηρετητή.



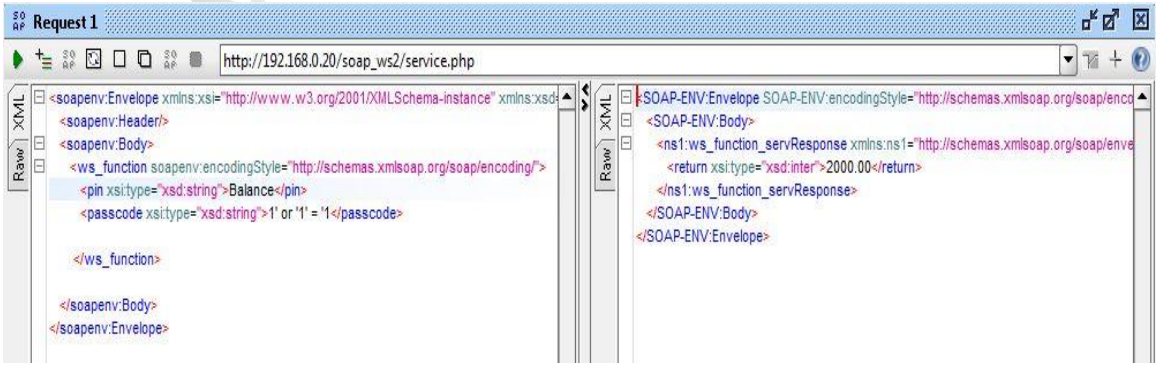
Εικόνα 42. Πινακάς TTP μετά από επιτυχή συναλλαγή των υπηρεσιών.

Με τη χρήση του εργαλείου SoapUI δημιουργούμε ένα νέο σχέδιο SOAP δίνοντας σαν παράμετρο τη διεύθυνση του WSDL αρχείου όπως φαίνεται στην παρακάτω εικόνα.



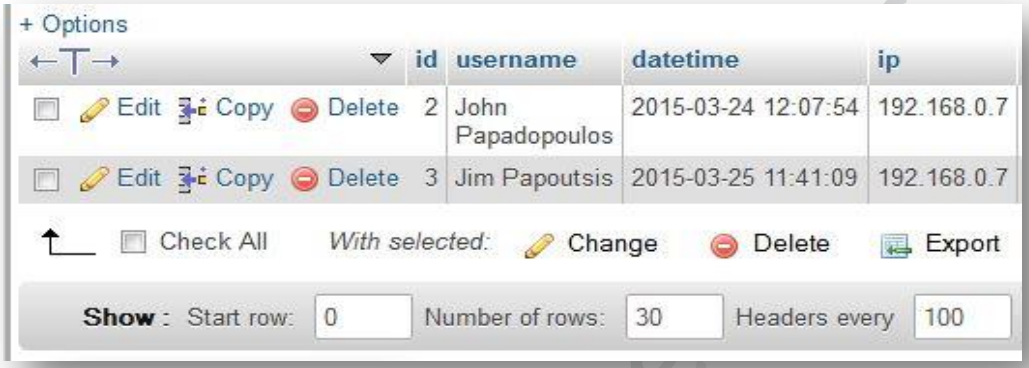
Εικόνα 43. Δημιουργία σχεδίου SOAP.

Εκτελώντας το αίτημα μέσω του SoapUI με παραμέτρους με τις οποίες μια βάση δεδομένων θεωρείται ευάλωτη σε Sql Injection επιθέσεις επιστρέφεται απάντηση με το υπόλοιπο ενός λογαριασμού.



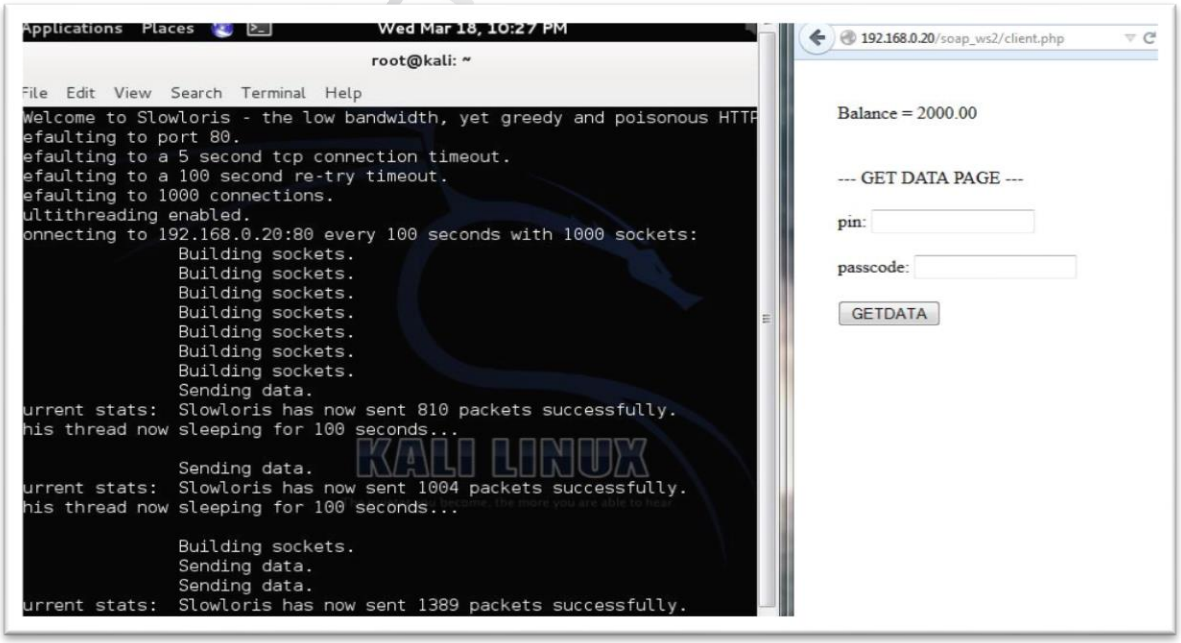
Εικόνα 44. Επίθεση Sql Injection με τη χρήση SoapUI.

Μελετώντας τα αρχεία καταγραφής του TTP διακομιστή γίνεται αντιληπτό ότι η εν λόγω επίθεση δεν ανιχνεύθηκε και το αρχείο καταγραφής της βάσης δεδομένων του TTP δεν περιέχει καμία εγγραφή και πληροφορία για την επίθεση αυτή. Γίνεται εύκολα αντιληπτό ότι ο έλεγχος και οι αυτοματισμοί που δημιουργήθηκαν με την παρουσία του TTP διακομιστή δεν επαρκούν για τον εντοπισμό της επίθεσης ή την καταγραφή αυτών των πληροφοριών που θα αποτελούν πειστήρια για μια εγκληματολογική Δικανική έρευνα.



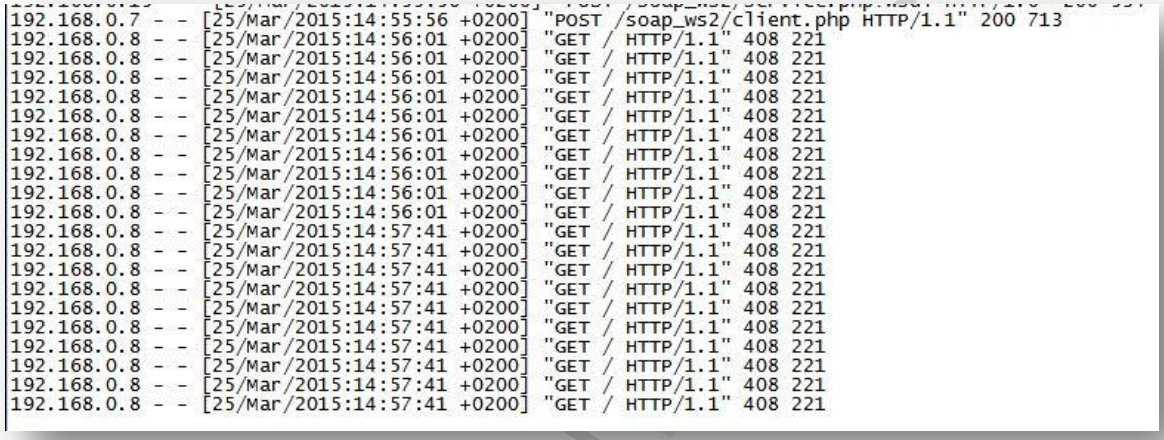
Εικόνα 45. Μη καταγραφή της επίθεσης στον πίνακα δεδομένων του TTP διακομιστη.

Επίθεση άρνησης υπηρεσιών: Με τη χρήση του εργαλείου SlowLoris στο πείραμα του πρώτου σεναρίου δεν ήταν δυνατό να αντιμετωπιστούν επιθέσεις άρνησης υπηρεσιών από το υπάρχων τεχνολογικό περιβάλλον. Έχοντας εγκαταστήσει και δημιουργώντας τους κατάλληλους κανόνες στο εργαλείο mod_antiloris βλέπουμε ότι επιθέσεις DoS είναι δυνατό να αντιμετωπιστούν με αποτελεσματικό τρόπο.



Εικόνα 46. Η υπηρεσία συνεχίζει να είναι ενεργή μετά από την επίθεση άρνησης υπηρεσιών.

Παρόλα αυτά αν ένας ειδικός ερευνητής αναζητήσει αποδεικτικά στοιχεία για το είδος της επίθεσης στο αρχείο καταγραφής του Apache παρουσιάζεται μόνο μια διεύθυνση IP που αποστέλλει αρκετά αιτήματα προς την υπηρεσία (συγκεκριμένα η διεύθυνση IP 192.168.0.8) κάτι που δεν θα αποτελούσε αξιόπιστο πειστήριο στο οποίο θα μπορούσε να στηριχτεί Δικανική έρευνα. Ακόμα στο αρχείο καταγραφής εμφανίζεται η διεύθυνση IP του «νόμιμου» χρήστη που χρησιμοποίησε την υπηρεσία ιστού (192.168.0.7).



Εικόνα 47. Αρχείο καταγραφής Apache διακομιστή με την επίθεση άρνησης υπηρεσιών.

<u>Σενάριο 3^{ο}</u> : Όπως παρατηρήσαμε στα δύο προηγούμενα παραδείγματα, παρόλα τα αντίμετρα που εφαρμόστηκαν δεν κρίθηκαν αρκετά για να προστατέψουν τις υπηρεσίες ιστού από επιθέσεις ή να συλλέξουν όλα τα απαραίτητα δεδομένα με τα οποία ένας ερευνητής της Δικανικής πληροφορικής θα είχε την δυνατότητα να τα συλλέξει, να τα αναλύσει έτσι ώστε να ανακατασκευάσει το συμβάν της επίθεσης και τέλος να παρουσιάσει όλα τα απαραίτητα πειστήρια στις Δικαστικές αρχές με αποτέλεσμα να αποδοθούν κυρώσεις στους ψηφιακούς εγκληματίες.

Μια από τις μεγαλύτερες παραλείψεις των προηγούμενων παραδειγμάτων είναι η μη ύπαρξη μιας μεθόδου όπου θα προλαμβάνει περιστατικά επιθέσεων και θα παρέχει ένα πλαίσιο εργασιών που θα ορίζει όλες τις αρμοδιότητες των εμπλεκόμενων μερών, τον τρόπο που θα γίνονται οι προειδοποιήσεις όταν υπάρχει ένα συμβάν επίθεσης, οι αυτοματισμοί και τα εργαλεία που θα καταγράφουν και θα αποτρέπουν τέτοιου είδους ηλεκτρονικών επιθέσεων, καθώς επίσης και το πώς θα πρέπει να συλλεχθούν και θα αναλυθούν τα απαραίτητα δεδομένα που θα αποτελούν τα αποδεικτικά στοιχεία της Δικανικής έρευνας με απώτερο στόχο να αποδοθούν ευθύνες.

Στο 3^{ο} σενάριο κατά σειρά που θα παρουσιαστεί θα γίνει η εφαρμογή των βημάτων της βέλτιστης μεθοδολογίας που περιγράφηκε στην ενότητα 3.2.4 έτσι ώστε στο τέλος να αξιολογηθεί το αποτέλεσμα του πειράματος συνολικά με την εφαρμογή μιας μεθοδολογίας Δικανικής πληροφορικής που αποσκοπεί κυρίως στη προστασία των υπηρεσιών του ιστού ενός οργανισμού.

Φάση 1

Σε αυτή τη φάση θα πρέπει να γίνει λήψη όλων των προληπτικών μέτρων (proactive) έτσι ώστε να εξασφαλισθεί με αυτοματισμούς και τεχνολογικά εργαλεία ανίχνευση και η αποτροπή των ηλεκτρονικών επιθέσεων έναντι στις υπηρεσίες του πληροφοριακού συστήματος.

Πρώτο βήμα: Μελετώντας το τεχνολογικό περιβάλλον ένας ειδικός επιστήμονάς εντοπίζει τις ευπάθειες στις υπηρεσίες ιστού που παρέχονται και δεν μπόρεσαν να αντιμετωπιστούν στα προηγούμενα παραδείγματα. Θα πρέπει να δημιουργηθούν οι κατάλληλες προσθήκες στον διακομιστή TTP έτσι ώστε να είναι δυνατό να ανιχνεύονται και να αποτρέπονται οι επιθέσεις Sql Injection καθώς επίσης να καταγράφονται τέτοιου είδους συναλλαγές. Στο κομμάτι των επιθέσεων άρνησης υπηρεσιών (DoS attacks), στα προηγούμενα παραδείγματα αντιμετωπίστηκε αποτελεσματικά μια τέτοιου είδους επίθεση αλλά δεν υπήρχαν τα απαραίτητα πειστήρια που θα υποδείκνυε ότι το σύστημα δέχτηκε επίθεση, κάτι που καθιστά απαραίτητη την ανάγκη ύπαρξης ενός εργαλείου καταγραφής (log) για μια τέτοια επίθεση.

Δεύτερο βήμα: Σε αυτό το βήμα γίνεται η ανάθεση των αρμοδιοτήτων. Οι διαχειριστές των τεχνολογικών συστημάτων του οργανισμού είναι οι υπεύθυνοι για τη συντήρηση, διαχείριση και ενημέρωση όλου τεχνολογικού περιβάλλοντος. Είναι υποχρεωμένοι να επιβλέπουν όλα τα Δικανικά εργαλεία και σε περίπτωση επίθεσης να λειτουργούν αναλόγως και να επικοινωνούν με τα κατάλληλα άτομα για την διαχείριση του κινδύνου. Αναλαμβάνουν ακόμα και την εκπαίδευση των απλών χρηστών για την ορθή και ασφαλή λειτουργία των υπηρεσιών. Ο υπεύθυνος του τμήματος πληροφορικής, τέλος είναι υπεύθυνος να επικοινωνήσει και να δώσει όλες τις απαραίτητες πληροφορίες και δικαιώματα πρόσβασης στους ερευνητές της Δικανικής εγκληματολογίας μετά από ένα συμβάν ψηφιακής επίθεσης.

Τρίτο βήμα: Με τις υποδείξεις του ειδικού ερευνητή γίνονται οι απαραίτητες αλλαγές έτσι ώστε το πληροφοριακό σύστημα να γίνει πιο ασφαλές. Στο τρίτο βήμα της πρώτης φάσης της βέλτιστης μεθοδολογίας, θα εφαρμοστούν οι απαραίτητες αλλαγές στο περιβάλλον των υπηρεσιών ιστού έτσι ώστε να διασφαλιστεί η ορθή λειτουργία των υπηρεσιών, να αποτραπούν κακόβουλες επιθέσεις και να εξασφαλιστεί η διαθεσιμότητα των υπηρεσιών αυτών.

Βάση των αποτελεσμάτων των προηγούμενων σεναρίων κρίνεται απαραίτητο να γίνει προσθήκη μια επιπλέον λειτουργίας (function) κατά την οποία η τελική υπηρεσία service_ws θα ελέγχει εάν η κλήση που δέχθηκε προέρχεται από το TTP διακομιστή, δηλαδή από το ασφαλές κανάλι επικοινωνίας και όχι από κάποια άγνωστη διεύθυνση IP. Για να επιτευχθεί αυτό θα πρέπει να προστεθούν κάποιες επιπλέον λειτουργίες τόσο στο κομμάτι του TTP διακομιστή όσο και στο κομμάτι της τελικής υπηρεσίας (endpoint). Όπως παρουσιάζεται και στο κώδικα που ακολουθεί, η τελική υπηρεσία στην λειτουργία της περιλαμβάνει κάποιους πρόσθετους ελέγχους. Σε μια μεταβλητή *$callerIP* καταγράφεται η απομακρυσμένη IP του χρήστη ή της εφαρμογής που κάλεσε την υπηρεσία ιστού. Στη συνέχεια γίνεται έλεγχος αν η διεύθυνση του αποστολέα είναι αυτή του TTP διακομιστή, στο παράδειγμα της πειραματικής διαδικασίας θεωρούμε ότι ο TTP διακομιστής έχει IP διεύθυνση *192.168.0.15*. Αν επαληθευτεί η διεύθυνση του TTP τότε η τελική υπηρεσία αποστέλλει τα ζητούμενα δεδομένα και με την σειρά του ο TTP διακομιστής τα μεταβιβάζει στον πελάτη (client).

```
function ws_function_serv($pin,$passcode){
        //ανίχνευση IP για έλεγχο αν ανήκει στο TTP server ή σε επιτιθέμενο
        $callerIP = $_SERVER['REMOTE_ADDR'];
        //έλεγχος αν η κλήση προέρχεται από τον TTP
                if($callerIP == "192.168.0.15"){
                //δεδομένα από τη βάση (bank) σύμφωνα με τα στοιχεία εισόδου χρηστή (pin and passcode)
                $sql = "select * from bank where pin='".$pin."' and passcode='".$passcode."'";
                $run =  mysql_query($sql) or die(mysql_error());
                if(mysql_num_rows($run)>0){
                        $row = mysql_fetch_assoc($run);
                        $balance = $row['balance']; //υπόλοιπο λογαριασμού χρήστη
                } else {
                        $balance = "Wrong pin/passcode";                    }
                return $balance;
        }
```

Αν κατά τον έλεγχο ανιχνευτεί μια IP διεύθυνση διαφορετική από αυτή του TTP τότε δημιουργείται μια νέα μεταβλητή *$client* η οποία αναλαμβάνει να καλέσει και να στείλει ένα σύνολο παραμέτρων στην υπηρεσία ιστού του TTP. Οι παράμετροι που θα αποσταλούν είναι: η IP η οποία θεωρείται σαν ύποπτη, τα “pin” και “passcode που δίνονται σαν δεδομένα εισόδου από τη συγκεκριμένη IP, καθώς και η χρονική στιγμή που έγινε η κλήση προς την υπηρεσία. Τέλος, καλείται η *“ws_function_ttp_intrusion”* υπηρεσία του TTP και αποστέλλονται όλες οι προαναφερθείσες παράμετροι. Παρακάτω παρουσιάζεται μέρος του κώδικα.

```
else {
$wsCallDatetime = date("Y",time())."-".date("m",time())."-".date("d",time())."
".date("H",time()).":".date("i",time()).":".date("s",time());
//δημιουργία νέου πελάτη για τη TTP υπηρεσία ιστού
                $client = new nusoap_client("http://192.168.0.15/soap_ws3/ttp.php?wsdl");
        //κλήση της λειτουργίας TTP, αποστολή παραμέτρων
                $client->call('ws_function_ttp_intrusion', $params);
        }
```

Όταν κληθεί η υπηρεσία *"ws_function_ttp_intrusion"* ο TTP διακομιστής προσθέτει στο αρχείο καταγραφής της βάσης δεδομένων του τα δεδομένα του επιτιθέμενου που του έχουν αποσταλεί, όπως φαίνεται στη λειτουργία του κώδικα που ακολουθεί. Στην Εικόνα 48 παρουσιάζεται η νέα δομή του πίνακα ttp. Αξίζει να σημειωθεί ότι το πεδίο "intrusion_detected" λειτουργεί σαν «διακόπτης», δηλαδή σε περίπτωση που ανιχνευτεί μια επίθεση παίρνει την τιμή "1"αλλιώς έχει την προεπιλεγμένη τιμή "0".

```
function ws_function_ttp_intrusion($pin,$passcode,$ip,$datetime){

        //προσθήκη αρχείου καταγραφής στη βάση

        $sql = "insert into ttp (pin, passcode, ip, datetime,
intrusion_detected) values
('".$pin."','".$passcode."','".$ip."','".$datetime."',1)";

        $run = mysql_query($sql) or die(mysql_error());

}
```

	id	username	datetime	ip	pin	passcode	intrusion_detected
Copy Delete	2	John Papadopoulos	2015-03-24 12:07:54	192.168.0.7	NULL	NULL	0
Copy Delete	3	Jim Papoutsis	2015-03-25 11:41:09	192.168.0.7	NULL	NULL	0

Εικόνα 48. Δομή του πίνακα ttp με τα πεδία "pin","passcode","intrusion_detected".

Στο δεύτερο πειραματικό σενάριο έγινε χρήση του εργαλείου mod_antiloris, παρόλο που το συγκεκριμένο εργαλείο δρα αποτελεσματικά σε επιθέσεις άρνησης υπηρεσιών δεν παρέχει όλα τα δεδομένα που ένας ειδικός εγκληματολογικός ερευνητής θα μπορούσε να παρουσιάσει στις Δικαστικές αρχές. Συμπληρωματικά με τη λειτουργία του mod_antiloris προστίθεται το εργαλείο mod_security2. Το mod_security2 έχει τη λειτουργία ενός μηχανισμού αντιμετώπισης περιστατικών (Incident Response) συμπληρώνοντας τη λειτουργία του mod_antiloris το οποίο αποτελεί σύστημα ανίχνευσης εισβολής (Intrusion Detection System). Το mod_security2 μέσω από ένα σύνολο κανόνων μπορεί να καταγράψει σε ένα αρχείο καταγραφών (log file) ότι το σύστημα δέχεται επιθέσεις τύπου άρνησης υπηρεσιών. Το mod_security2 θα πρέπει να εγκατασταθεί στο φάκελο *"modules"* του Apache διακομιστή και βασική προϋπόθεση είναι η ύπαρξη των βιβλιοθηκών *"libxml2.dll"*[29] *και "yajl.dll"* στο φάκελο "*bin*" του Apache. Στη συνέχεια θα πρέπει το Το mod_security2 να «φορτωθεί» στο αρχείο "httpd.conf" του Apache όπως φαίνεται στη παρακάτω εικόνα.

[29] Θα πρέπει επίσης να φορτωθούν το module unique_id. Προτείνεται η φόρτωση του mod_security2 να προηγείται του mod_antiloris.

```
LoadModule security2_module modules/mod_security2.so

<IfModule security2_module>
SecRuleEngine On
SecDebugLog "c:/wamp/mod-security.log"
SecDebugLogLevel 6
SecReadStateLimit 10
SecWriteStateLimit 10
</IfModule>
```

Εικόνα 49. Φόρτωση του mod_security2.so

Στην Εικόνα 49 εμφανίζονται οι κανόνες του mod_security2 που θα εφαρμοστούν στην πειραματική διαδικασία. Με τη χρήση του κανόνα "*SecRuleEngine On*" γίνεται εκκίνηση της βιβλιοθήκης κανόνων του mod_security2. Στη συνέχεια δίνουμε τη διαδρομή που θα αποθηκεύεται το αρχείο καταγραφής του mod-security, με την ονομασία "mod-security.log", με τη εντολή "*SecDebugLogLeve 6*" δίνουμε τη ρύθμιση να καταγράφονται όλες οι συναλλαγές των υπηρεσιών ιστού. Τέλος, με τους κανόνες "*SecConnReadStateLimit 10*" και "*SecConnWriteStateLimit 10*" καθορίζουμε ότι τα όρια των ταυτόχρονων συνδέσεων σε κατάσταση ανάγνωσης και εγγραφής στο Apache διακομιστή δεν θα ξεπερνάνε τις δέκα συνδέσεις ανά IP διεύθυνση. Επισημαίνεται ότι οι κανόνες του mod_antiloris παραμένουν οι ίδιοι με το σενάριο 2 και παρουσιάζονται στην παρακάτω εικόνα.

```
LoadModule security2_module modules/mod_security2.so

<IfModule security2_module>
SecRuleEngine On
SecDebugLog "c:/wamp/logs/mod-security.log"
SecDebugLogLevel 6
SecConnReadStateLimit 10
SecConnWriteStateLimit 10
</IfModule>
```

Εικόνα 50. Κανόνες του εργαλείου mod_security2.

Τέταρτο βήμα: Σε αυτό το βήμα καθορίζονται οι αρμοδιότητες των εξωτερικών εγκληματολόγων της Δικανικής πληροφορικής. Οι ειδικοί εγκληματολόγοι έχουν την ευθύνη αρχικά να υποδείξουν όλες τις ευπάθειες των υπηρεσιών του οργανισμού έτσι ώστε να εγκατασταθούν τα κατάλληλα Δικανικά εργαλεία για την αντιμετώπιση ψηφιακών επιθέσεων και την καταγραφή αυτών των συναλλαγών που έχουν εγκληματολογική αξία. Σε κάθε περίπτωση που ανιχνεύεται μια κακόβουλή επίθεση καλούνται από τους διαχειριστές των τεχνολογικών συστημάτων να συλλέξουν και να αναλύσουν τα δεδομένα της επίθεσης, έχοντας πλήρη πρόσβαση στα συστήματα που έχουν επηρεαστεί. Τέλος, αναλαμβάνουν να παρουσιάσουν εγγράφως τα αποτελέσματα της έρευνας στις Δικαστικές αρχές.

Πέμπτο βήμα: Στο εν λόγω βήμα γίνεται η έγγραφη επικύρωση όλων αυτών των διαδικασιών που θα ακολουθηθούν κατά τη διάρκεια μιας έρευνας.

Φάση 2

Η δεύτερη φάση του τρίτου σεναρίου αφορά τη ανίχνευση ενός συμβάντος ηλεκτρονικής επίθεσης και ποια είναι τα βήματα και οι ενέργειες που θα γίνουν από τη στιγμή που θα ανιχνευτεί η επίθεση αυτή. Για τη συνέχεια της πειραματικής διαδικασίας πραγματοποιούμε τις δύο επιθέσεις των προηγούμενων σεναρίων, αυτών του Sql Injection και της άρνησης υπηρεσιών.

Επίθεση Sql Injection : Για τη συνέχεια της πειραματικής διαδικασίας θεωρούμε ότι ο επιτιθέμενος θα έχει IP διεύθυνση 192.168.0.8. Χρησιμοποιώντας την εντολή "*perl slowloris.pl –dns 192.168.0.20 –port 80 –timeout 30 –num 500"* στέλνουμε αιτήματα στην πόρτα 80 της IP 192.168.0.20 κάθε είκοσι δευτερόλεπτα για 500 sockets. Στην εικόνα που ακολουθεί παρουσιάζεται η επιτυχής αποστολή των πακέτων.

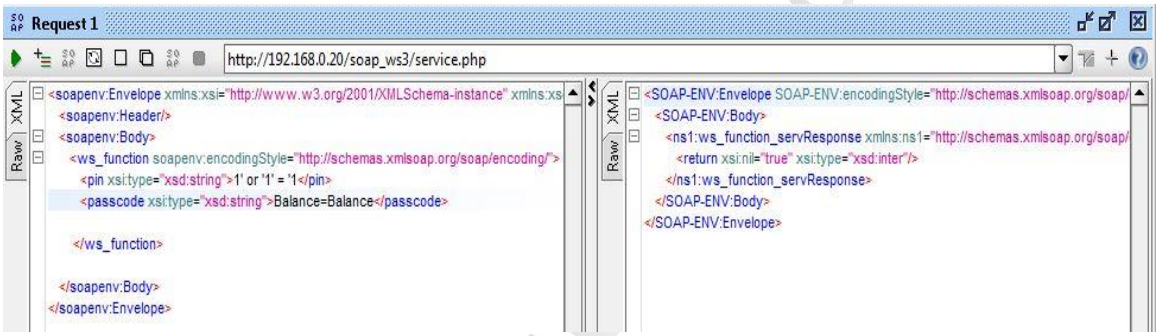
Εικόνα 51. Επίθεση με το εργαλείο στον διακομιστη υπηρεσιών ιστού SlowLoris.

Επίθεση Sql Injection : Με τη χρήση του εργαλείου SoapUI, ο επιτιθέμενος του προηγούμενου παραδείγματος με διεύθυνση IP 192.168.0.8 επιχειρεί να υποκλέψει δεδομένα από τη βάση της υπηρεσίας εκμεταλλευόμενος την ευπάθεια σε Sql Injection και γνωρίζοντας τη διεύθυνση του WSDL αρχείου "*http://localhost/soap_ws3/service.php?wsdl"*. Στις εικόνες που ακολουθούν ο επιτιθέμενος προσπαθεί να δώσει διάφορε τιμές έτσι ώστε να επιτύχει το επιθυμητό αποτέλεσμα. Αρχικά δίνει τις τιμές εισόδου:

- pin: "*Give Balance*" και passcode: "*1' or '1' = '1*".
- pin: "*1' or '1' = '1*" και passcode: "*Balance=Balance*".

Παρατηρώντας τις εικόνες και στις δύο περιπτώσεις δεν επιστρέφονται αποτελέσματα στον επιτιθέμενο όπως συνέβαινε στα δύο πρώτα σενάρια.

Εικόνα 52. Επίθεση 1η pin: "Give Balance" και passcode: "1' or '1' = '1".



Εικόνα 53. Επίθεση 2η pin: "1' or '1' = '1" και passcode: "Balance=Balance".

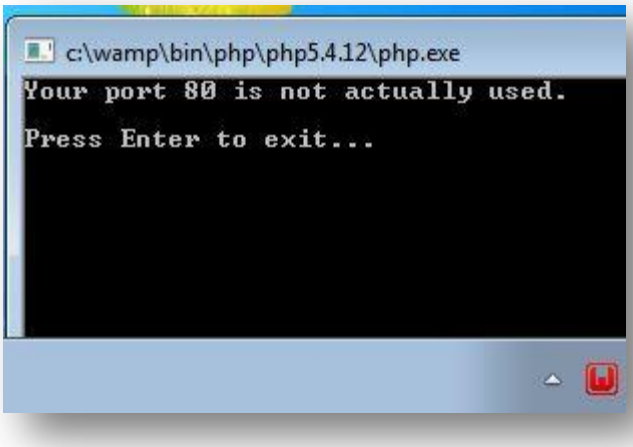
Πρώτο βήμα: Στο πρώτο βήμα της δεύτερης φάσης, οι διαχειριστές των συστημάτων του πληροφοριακού συστήματος ενημερώνονται από το mod_security2 ότι το σύστημα δέχθηκε επίθεση άρνησης υπηρεσιών.

[:warn] [pid 1728:tid 1744] ModSecurity: Access denied with code 400. Too many threads [1920] of 10 allowed in READ state from 192.168.0.8 - Possible DoS Consumption Attack [Rejected]

[:warn] [pid 1728:tid 1744] ModSecurity: Access denied with code 400. Too many threads [1920] of 10 allowed in READ state from 192.168.0.8 - Possible DoS Consumption Attack [Rejected]

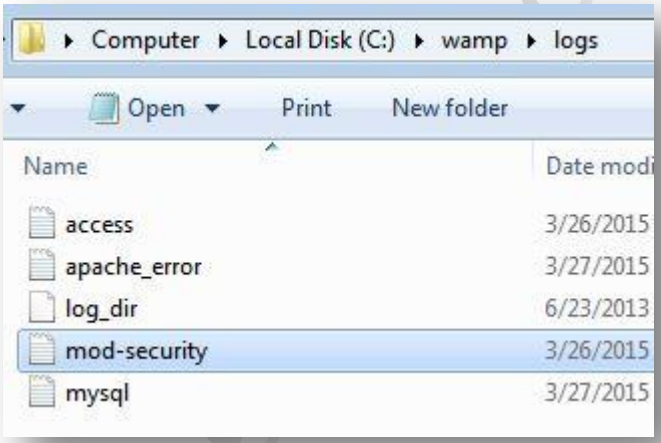
Παρατηρούμε σύμφωνα με το αρχείο καταγραφών ότι ο χρήστης με IP 192.168.0.8 επιχείρησε πολλά και συνεχόμενα αιτήματα προς την υπηρεσία. Το mod_security2 εργαλείο θεώρησε τη συναλλαγή αυτή σαν μια πιθανή επίθεση άρνησης υπηρεσιών και τη απέρριψε. Η επόμενη ενέργεια των υπεύθυνων των συστημάτων είναι να ειδοποιήσουν τους ερευνητές της Δικανικής πληροφορικής έτσι ώστε να εξετάσουν το συμβάν.

Δεύτερο βήμα: Στο εν λόγω βήμα οι ειδικοί ερευνητές έχοντας τις απαραίτητες εξουσιοδοτήσεις και προσβάσεις στα συστήματα του οργανισμού, εντοπίζουν ότι η επίθεση αφορά τις υπηρεσίες ιστού και απομονώνουν το πληροφοριακό περιβάλλον σταματώντας προσωρινά την τελική υπηρεσία έτσι ώστε να ξεκινήσει η συλλογή των δεδομένων της επίθεσης. Η επόμενη ενέργεια των ειδικών ερευνητών είναι να θέσουν σε κατάσταση αναμονής τον Apache διακομιστή του οργανισμού.



Εικόνα 54.Αδρανοποίηση του Apache διακομιστή για την έναρξη συλλογής πειστηρίων.

Τρίτο βήμα: Στο τρίτο κατά σειρά βήμα οι ερευνητές της Δικανικής εγκληματολογίας αναζητούν τα δεδομένα αυτά που θα αποτελέσουν τα αποδεικτικά στοιχεία της έρευνας έχοντας σαν σημείο εκκίνησης το αρχείο καταγραφής (log file) του Apache και τις ειδοποιήσεις του εργαλείου mod_security2 συλλέγουν τα αρχεία καταγραφής από το φάκελο "*log"* του Apache: access, apache_error,mod-security και mysql.



Εικόνα 55. Χώρος αποθήκευσης αρχείων καταγραφών.

Στη συνέχεια από τη βάση δεδομένων "*soap_ws"* και τον πίνακα "*ttp"* γίνεται η εξαγωγή των δεδομένων που έχει καταγράψει ο TTP διακομιστής. Τέλος, όλα τα δεδομένα αυτά φυλάσσονται από τους ειδικούς ερευνητές και καταγράφονται στη λίστα των «εξαγόμενων δεδομένων».

	id	username	datetime	ip	pin	passcode	intrusion_detected
Edit Copy Delete	2	John Papadopoulos	2015-03-24 12:07:54	192.168.0.7	NULL	NULL	0
Edit Copy Delete	5	Jim Papoutsis	2015-03-25 12:55:49	192.168.0.7	NULL	NULL	0
Edit Copy Delete	8	NULL	2015-03-26 21:44:49	192.168.0.8	Give Balance	1' or '1' = '1	1
Edit Copy Delete	9	NULL	2015-03-26 21:45:07	192.168.0.8	1' or '1' = '1	Balance=Balance	1

Check All With selected: Change Delete Export

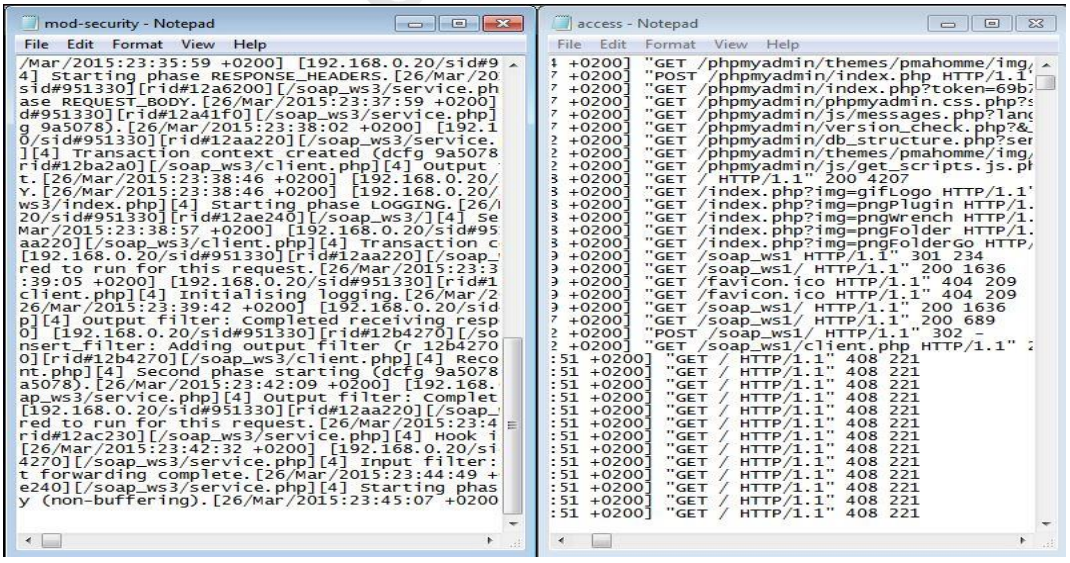
Εικόνα 56. Εξαγωγή δεδομένων από τον πίνακα ttp.

Τέταρτο βήμα: Στο εν λόγω βήμα γίνεται η ανάλυση των δεδομένων τα οποία συλλέχθηκαν στο προηγούμενο βήμα. Τα δεδομένα αυτά που αποτελούν πειστήρια τοποθετούνται στη λίστα «σχετικών δεδομένων». Στη λίστα «σχετικών δεδομένων» προστίθεται αρχικά τα δεδομένα από το αρχείο καταγραφής apache_error, καθώς καταγράφεται η IP διεύθυνση του πιθανόν επιτιθέμενου όπως και το είδος της επίθεσης.

[:warn] [pid 1728:tid 1744] ModSecurity: Access denied with code 400. Too many threads [1920] of 10 allowed in READ state from 192.168.0.8 - Possible DoS Consumption Attack [Rejected]

[:warn] [pid 1728:tid 1744] ModSecurity: Access denied with code 400. Too many threads [1920] of 10 allowed in READ state from 192.168.0.8 - Possible DoS Consumption Attack [Rejected]

Αναλύοντας τα αρχεία καταγραφής mod-security.log και access.log δείχνουν να περιέχουν δεδομένα από «νόμιμες» συναλλαγές μεταξύ των πελατών και των υπηρεσιών ιστού. Τα συγκεκριμένα δεδομένα δεν θα προστεθούν στη λίστα «σχετικών δεδομένων».



Εικόνα 57. Δεδομένα access.log και mod-security.log.

Επιπροσθέτως τα δεδομένα του αρχείου καταγραφής mysql κρίνονται ότι δεν σχετίζονται με το συμβάν της επίθεσης. Στη συνέχεια εξετάζοντας τα εξαγόμενα δεδομένα από τον πίνακα ttp,παρατηρούμε ότι ο χρήστης με IP 192.168.0.8 κάλεσε την υπηρεσία ιστού δίνοντας τις τιμές pin:"*Give Balance*" - passcode: "*1' or '1' = '1*" και pin:"*1' or '1' = '1*" - passcode: "*Balance=Balance*" εισόδου σε κοντινές χρονικές στιγμές, έτσι ώστε να του επιστραφούν κάποια αποτελέσματα,. Ακόμα στο πεδίο "intrusion_detected" του πίνακα ttp παρατηρούμε ότι οι συγκεκριμένες εγγραφές έχουν την τιμή "1", δηλαδή έχει ανιχνευτεί και έχει καταγραφεί από το TTP διακομιστή συναλλαγή από το μη ασφαλές κανάλι επικοινωνίας μεταξύ των υπηρεσιών. Τέλος, μόνο τα δεδομένα του TTP διακομιστή με κωδικούς id: 8 και 9 προστίθενται στη λίστα «σχετικών δεδομένων» εφόσον οι χρήστε με id: 2 και 5 δείχνουν να έχουν νόμιμη πρόσβαση στην υπηρεσία. Η έρευνα προχωράει στο 5^{ο} βήμα καθώς δεν προέκυψαν νέα δεδομένα από την επεξεργασία των πειστηρίων που παρουσιάστηκαν.

id	username	datetime	ip	pin	passcode	intrusion_detected
2	John Papadopoulos	24/03/2015 12:07	192.168.0.7	NULL	NULL	0
8	NULL	26/03/2015 21:44	192.168.0.8	Give Balance	1' or '1' = '1	1
5	Jim Papoutsis	25/03/2015 12:55	192.168.0.7	NULL	NULL	0
9	NULL	26/03/2015 21:45	192.168.0.8	1' or '1' = '1	Balance=Balance	1

Εικόνα 58. Εξαγόμενο αρχείο από τη βάση δεδομένων soap_ws του πίνακα ttp.

id	username	datetime	ip	pin	passcode	intrusion_detected
2	John Papadopoulos	2015-03-24 12:07:54	192.168.0.7	*NULL*	*NULL*	0
5	Jim Papoutsis	2015-03-25 12:55:49	192.168.0.7	*NULL*	*NULL*	0
8	*NULL*	2015-03-26 21:44:49	192.168.0.8	Give Balance	1' or '1' = '1	1
9	*NULL*	2015-03-26 21:45:07	192.168.0.8	1' or '1' = '1	Balance=Balance	1

Εικόνα 59. Εικόνα της του πίνακα ttp μετά το συμβάν της επίθεσης, στη στήλη intrusion_detection διακρίνονται οι επιθέσεις με την τιμή "1".

Πέμπτο βήμα: Στο πέμπτο βήμα της πειραματικής διαδικασίας οι ειδικοί εγκληματολόγοι προσπαθούν να ανακατασκευάσουν το συμβάν της επίθεσης βάσει των δεδομένων της λίστας «σχετικών δεδομένων» που έχουν συλλεχθεί στο 4^{ο} βήμα.

Τα αποδεικτικά στοιχεία που έχουν συλλεχθεί από τις υπηρεσίες ιστού περιλαμβάνουν όλες τις προϋποθέσεις οι οποίες περιγράφονται στη βέλτιστη μεθοδολογία:

- Περιέχονται αποδεικτικά στοιχεία προέλευσης του επιτιθέμενου, όπως η διεύθυνση IP 192.168.0.8.

- Αποδεικτικά στοιχεία παράδοσης, εδώ μπορούν να αναφερθούν οι τιμές εισόδου που έδωσε ο κακόβουλος χρήστης προς τις υπηρεσίες ιστού έτσι ώστε να του επιστραφούν αποτελέσματα. Στο συγκεκριμένο παράδειγμα είναι οι τιμές pin:"*Give Balance*" - passcode: "*1' or '1' = '1*" και pin:"*1' or '1' = '1*" - passcode: "*Balance=Balance*".
- Τα στοιχεία του χρήστη της υπηρεσίας ιστού, ΄στο εν λόγω παράδειγμα το πεδίο username για τους χρήστες με id: 2 και 5 είναι «κενό» ("Null"), κάτι που παραπέμπει σε μη εξουσιοδοτημένη χρήση της υπηρεσίας και το πεδίο "datetime" του πίνακα περιγράφει τη χρονική στιγμή της αίτησης προς την υπηρεσία.
- Τα αρχεία καταγραφής έχουν ανιχνεύσει ότι το είδος της αρχικής επίθεσης αφορούσε επίθεση άρνησης υπηρεσιών (DoS) και στη συνέχεια από τα δεδομένα που εξάγονται από τον TTP διακομιστή παραπέμπουν σε απόπειρα επίθεσης Sql Injection.

Έχοντας αναλύσει τα δεδομένα που συλλέχθηκαν από τα διαθέσιμα εργαλεία, οι Δικανικοί ερευνητές ανακατασκευάζουν το συμβάν της επίθεσης. Σαν σημείο αναφοράς θεωρείται η καταγραφή του εργαλείου mod_security2 κατά την οποία ο χρήστης με IP 192.168.0.8 σε μια δεομένη χρονική στιγμή επιχείρησε ένα μεγάλο σύνολο κλήσεων προς την υπηρεσία έτσι ώστε να μπορέσει να καταστήσει αδύνατη στο να εξυπηρετήσει άλλα αιτήματα. Στη συνέχεια η ίδια IP διεύθυνση επιχείρησε να αντλήσει δεδομένα από τη βάση της υπηρεσίας τα οποία αφορούσαν τα υπόλοιπα λογαριασμών διαφόρων πελατών, εκμεταλλευόμενος την ευπάθεια της βάσης σε Sql Injection τεχνικές επίθεσης. Δίνοντας τις κατάλληλες τιμές ο επιτιθέμενος προσπαθεί να προσπελάσει τη βάση εκτός του ασφαλούς επικοινωνίας. Η κίνηση ανιχνεύεται και αποθηκεύεται στα αρχεία καταγραφής του TTP ενεργοποιώντας τους μηχανισμούς ειδοποίησης εισβολής και θέτοντας την τιμή "1" στο πεδίο intrusion_detected του σχετικού πίνακα. Όπως φαίνεται στην εικόνα που ακολουθεί έχει γίνει καταγραφή του χρόνου επίθεσης καθώς και των τιμών που θέλησε ο επιτιθέμενος να εισάγει στις υπηρεσίες (σε κάθε άλλη περίπτωση οι τιμές pin και passcode δεν καταγράφονται).

id	username	datetime	ip	pin	passcode	intrusion_detected
8	*NULL*	2015-03-26 21:44:49	192.168.0.8	Give Balance	1' or '1' = '1	1
9	*NULL*	2015-03-26 21:45:07	192.168.0.8	1' or '1' = '1	Balance=Balance	1

Εικόνα 60. Καταγραφή της κίνησης του επιτιθέμενου στη βάση δεδομένων του TTP διακομιστη.

Έκτο βήμα: Στο έκτο και τελευταίο βήμα της δεύτερης φάσης της βέλτιστης μεθοδολογίας, οι ειδικοί ερευνητές έχουν συλλέξει και αναλύσει όλα τα απαραίτητα αποδεικτικά στοιχεία με τα οποία μπορούν να υποδείξουν τον υπεύθυνο καθώς επίσης να δώσουν πλήρη περιγραφή του σεναρίου επίθεσης. Βάση των βημάτων που προηγήθηκαν οι Δικανική έρευνα έχει συλλέξει όλα τα απαραίτητα πειστήρια που υποδεικνύουν ότι ο χρήστης με IP διεύθυνση 192.168.0.8 είναι ο υπεύθυνος των ψηφιακών επιθέσεων.

Φάση 3

Πρώτο βήμα: Στο συγκεκριμένο πειραματικό περιβάλλον δεν υπάρχουν εναπομείναντα δεδομένα τα οποία αφορούν την δραστική ψηφιακή εγκληματολογία, αλλά η επίθεση εστιάζει στις υπηρεσίες ιστού του οργανισμού.

Δεύτερο βήμα: Στο δεύτερο βήμα γίνεται η αποκατάσταση των υπηρεσιών ιστού έτσι ώστε να είναι διαθέσιμες προς του χρήστες και να μην υπάρξουν επιπτώσεις σε ένα οργανισμό όπως οικονομικές επιπτώσεις.

Τρίτο βήμα: Σε συγκεκριμένο βήμα οι εγκληματολόγοι παραθέτουν μια τεκμηριωμένη έκθεση η οποία περιγράφει το συμβάν της επίθεσης, καθώς και όλα τα αποδεικτικά στοιχεία που υποδεικνύουν τον υπεύθυνο της επίθεσης, όπως αυτά παρουσιάστηκαν στο βήμα πέντε της δεύτερης φάσης της μεθοδολογίας. Τέλος, τεκμηριώνουν την έκθεση του παρουσιάζοντας όλο το αρχικό πλαίσιο της μεθοδολογίας που εφαρμόστηκε από τη πρώτη της φάση, όπως επίσης και τα προληπτικά μέτρα και εργαλεία που εγκαταστάθηκαν για να αποδειχθεί ότι το πληροφοριακό σύστημα που δέχτηκε την επίθεση πληροί όλες τις προϋποθέσεως της Δικανικής έρευνας και τα στοιχεία που συλλέγονται και αναλύονται είναι αξιόπιστα.

Τέταρτο βήμα: Στο τέταρτο βήμα της τρίτης φάσης της βέλτιστης μεθοδολογίας, γίνεται η παρουσίαση της έκθεσης στις Δικαστικές αρχές και βάσει των ισχυόντων νόμων ανακοινώνεται το τελικό πόρισμα και επιρρίπτονται οι ποινές στους υπεύθυνους της ηλεκτρονικής επίθεσης.

Στην ενότητα που ακολουθεί παρουσιάζεται η αξιολόγηση των αποτελεσμάτων από τα πειραματικά σενάρια που εφαρμόστηκαν.

4.4 Αξιολόγηση αποτελεσμάτων

Μετά το πέρας της πειραματικής διαδικασίας, συμπεραίνεται ότι η εφαρμογή των διαδικασιών και των εργαλείων της βέλτιστης μεθοδολογίας ενίσχυσε την προστασία των υπηρεσιών ιστού του τεχνολογικού περιβάλλοντος που παρουσιάστηκε και ασφάλισε την αξιοπιστία μιας ενδεχόμενης Δικανικής έρευνας. Οι ευπάθειες των δύο αρχικών σεναρίων καλύφθηκαν με το βέλτιστο τρόπο όχι μόνο από την εφαρμογή των διαφόρων αυτοματισμών αλλά και από ένα πλαίσιο βημάτων που επιτρέπουν την άμεση αντίδραση σε ένα συμβάν ψηφιακής επίθεσης. Τα βήματα της μεθοδολογίας ήταν ξεκάθαρα για κάθε φάση της έρευνας και βάση των κανονισμών της νομοθεσίας. Ακόμα προστατεύτηκε το τεχνολογικό περιβάλλον των υπηρεσιών ιστού θέτοντας το προσωρινά σε κατάσταση αναμονής.

Σαν ένα επιπλέον βήμα που θα ενδυνάμωνε την αποτελεσματικότητα μιας Δικανικής έρευνας θα μπορούσε να είναι η οριστική αντιμετώπιση των ευπαθειών των συστημάτων, τις οποίες προσπάθησε ο επιτιθέμενος να εκμεταλλευτεί, εφόσον αυτές οι «αδυναμίες» εμφανιστούν κατά τη διάρκεια της μιας εγκληματολογικής έρευνας.

5 Επίλογος

Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής έγινε προσπάθεια της πλήρης παρουσίασης των αρχών, των κυριότερων μεθοδολογιών και των εργαλείων που αφορούν το πεδίο της «Δικανικής Πληροφορικής» και συγκεκριμένα τις «Δικανικές υπηρεσίες ιστού (Web Forensics)».

Η πολυπλοκότητα και η ραγδαία ανάπτυξη των τεχνολογιών και των υπηρεσιών ιστού (web services) απαιτεί από τους σύγχρονους οργανισμούς να λάβουν όλα αυτά τα μέτρα που θα ικανά να αντιμετωπίσουν τέτοιου είδους ηλεκτρονικές επιθέσεις. Οι υπηρεσίες ιστού αποτελούν αναπόσπαστο κομμάτι της σύγχρονης πληροφορικής καθώς με τις μεθόδους και την ευελιξία τους παρέχουν μια πληθώρα δυνατοτήτων και αυτοματισμών στη λειτουργία ενός οργανισμού ή μιας εταιρείας έχοντας παράλληλα και οικονομικά οφέλη. Κρίνεται αναγκαίο να εφαρμόζονται όλες οι Δικανικές μεθοδολογίες και όλα τα Δικανικά εργαλεία σε κάθε υπηρεσία ιστού. Οι Δικανικές μεθοδολογίες θα πρέπει να πλαισιώνονται από τα άρτια νομοθετικά πλαίσια μιας χώρας άλλα και να διαχειρίζονται από κατάλληλα εκπαιδευμένους χρήστες. Η σημαντικότητα των πληροφοριών που διαχειρίζονται οι υπηρεσίες ιστού (web services) καθώς και ευρεία εφαρμογή τους σε ολοένα και περισσότερα τεχνολογικά περιβάλλοντα, καθιστά επιτακτική την ανάγκη τη διασφάλιση όλων αυτών των τεχνολογιών μέσω των συμβουλευτικών υπηρεσιών των ειδικών της Δικανικής πληροφορικής.

Συνοψίζοντας, αντικείμενο της παρούσας μεταπτυχιακής διατριβής είναι να γίνουν κατανοητές όλες οι βασικές έννοιες της Δικανικής πληροφορικής, οι νόμοι που την πλαισιώνουν και όλα τα εργαλεία που διευκολύνουν την εφαρμογή της. Στη συνέχεια παρουσιάζονται όλες οι μεθοδολογίες που βρίσκουν εφαρμογή στη Δικανική υπολογιστική και προτείνεται μια βέλτιστη μεθοδολογία η οποία εστιάζει στη προστασία των υπηρεσιών ιστού (web services). Τέλος, γίνεται αναλυτική πρακτική εφαρμογή της βέλτιστης μεθοδολογίας και αξιολόγηση της μέσω πρακτικών παραδειγμάτων που μπορούν να εφαρμοστούν από τον κάθε αναγνώστη σε ένα εικονικό περιβάλλον.

Βιβλιογραφία

1. Norton Cyber Crime. [Ηλεκτρονικό] http://us.norton.com/cybercrimereport/.

2. **CERT, US -.** Computer Forensics US-CERT. *Produced 2008 ;;;by US-CERT, a goverment organization.*

3. **LLC, McConnell International.** Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information. December 2000.

4.**http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&lang=.** *Μορφές Κυβερνοεγκλήματος.*

5. **https://msisac.cisecurity.org/resources/reports/documents/b-norton-report-2013.pdf.** *2013 NORTON REPORT .* 2013.

6. **Volkamer, Dieter Hutter and Melanie.** Preserving Privacy in Dynamic Web Service. *German Research Center for Artificial Intelligence (DFKI GmbH).*

7. *Information Security and Forensics Society, "Computer Forensics Part 2: Best ".* Μάιος2004.

8. **Ankit Agarwal, Megha Gupta, Saurabh Gupta & Prof. (Dr.) S.C. Gupta.** cscjournals. [Ηλεκτρονικό] http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJCSS-438.pdf.

9. **United States Department of Justice - Kenneth E. Melson.** [Ηλεκτρονικό] Ιανουάριος 2008. http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf.

10. **CP Grobler, CP Louwrens, SH von Solms.** *A multi-component view of Digital Forensics.* Johannesburg, South Africa : International Conference on Availability, Reliability and Security, 2010.

11. **Richardson, Robert.** *CSI Computer Crime & Security Survey.* 2008.

12. **Rouse, Margaret.** *http://searchsecurity.techtarget.com/definition/incident-response.* [Ηλεκτρονικό] September 2005.

13. **Grand, Brian D. Carrier-Joe.** *A Hardware-Based Memory Acquisition Procedure for Digital.* s.l. : Digital Investigation Journal, 2004.

14. **Alh, Soltan και arbi, Jens Weber-Jahnke, Issa Traore.** *The Proactive and Reactive Digital Forensics; Investigation Process: A SAystematic Literature Review.* s.l. : International Journal and its Applications, October,2011.

15. **Wikipedia.** *Apache HTTP εξυπηρετητής.* http://el.wikipedia.org/wiki/Apache_HTTP_%CE%B5%CE%BE%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%84%CE%B7%CF%84%CE%AE%CF%82.

16. **Ristić, Ivan.** *Ivan Ristić - mod_security.* http://blog.ivanristic.com/modsecurity/.

17. ΚΥΒΕΡΝΟΧΩΡΟΣ-ΤΟ ΔΙΕΘΝΕΣ «ΓΙΓΝΕΣΘΑΙ» ΣΤΟ ΕΛΛΗΝΙΚΟ «ΕΙΝΑΙ» Του Υπαστυνόμου Α΄ Δ.Π. ΑΓΓΕΛΟΠΟΥΛΟΥ Εξεταστεί Ψηφιακών Πειστηρίων Της Διεύθυνσης Εγκληματολογικών Ερευνών ΕΛ.ΑΣ.

18. Council of Europe. Computer Related Crime. http://www.oas.org/juridico/english/89-9&final%20Report.pdf

19. WS-Trust V1.0 Working Draft, OASIS Web Services Secure Exchange TC, http://www.oasisopen.org/committees/download.php/16138/oasis-wssx-ws-trust-1.0.pdf , 2006.

20. OASIS, WS-SecureConversation 1.3, 2007.

21. Τσουμάρης ΧΡ. , «Ψηφιακή Εγκληματικότητα. Η ανασφαλής όψη του Δικτύου», Εκδόσεις Βας. Ν. Κατσαρού, 2005.