ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: Ασφαλής ανάκτηση και ανάλυση δικτυακών δεδομένων – Network Forensics

Ελευθεριάδης Αθανάσιος
Μεταπτυχιακός Φοιτητής

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΑΥΡΙΔΗΣ ΙΩΑΝΝΗΣ, Επ. Καθηγητής

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Στειακάκης Εμμανουήλ , Λέκτορας
Αλεξανδροπούλου Ευγενία, Αναπ. Καθηγήτρια

Θεσσαλονίκη, Σεπτέμβριος 2011

Αφιερώνεται στη Σπυριδούλα
για την υπομονή και κατανόηση
κατά τη διάρκεια εκπόνησης
της παρούσας διπλωματικής εργασίας,
και στους γονείς μου.

Ευχαριστώ τον κ. Μαυρίδη Ιωάννη
για τις χρήσιμες συμβουλές του
και τη χρήσιμη βοήθεια για την εκπόνηση
της παρούσας διπλωματικής εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

0. Εισαγωγή 1
1. Forensics - Η Επιστήμη των Forensic 2
1.1 Κλάδοι των forensics 2
1.1.1 Επιστήμες Φυσιολογίας 2
1.1.1.1 Δικανική Ανθρωπολογία 3
1.1.1.2 Δικανική Αρχαιολογία 3
1.1.1.3 Δικανική Οδοντιατρική 4
1.1.1.4 Δικανική Εντομολογία 5
1.1.1.5 Δικανική Παθολογία 5
1.1.2 Κοινωνικές Επιστήμες 5
1.1.2.1 Δικανική Ψυχολογία και Ψυχιατρική 6
1.1.3 Εγκληματολογία 6
1.1.3.1 Βαλλιστική 6
1.1.3.2 Γενετική 7
1.1.3.3 Δακτυλοσκοπία 7
1.1.3.4 Ποδιατρική 8
1.1.3.5 Τοξικολογία 8
1.1.4 Ψηφιακή Δικανική 9
1.1.4.1 Δικανική Υπολογιστών 10
1.1.4.2 Δικανική Κινητών Συσκευών 10
1.1.4.3 Δικανική Δικτύων 11
1.1.5 Σύγκριση της Δικανικής Δικτύων και των Συστημάτων Ανίχνευσης Παρείσφρησης 13
1.1.6 Άλλοι κλάδοι των forensics που δεν εμπίπτουν στις παραπάνω κατηγορίες 14
2. Μεθοδολογία 15
2.1 Μεθοδολογία της Ψηφιακής Δικανικής 15
2.1.1 Απόκτηση των στοιχείων 15
2.1.2 Αλυσίδα Φύλαξης 16
2.2 Ένα γενικό πλαίσιο για τη Δικανική Δικτύων 17
2.2.1 Προετοιμασία και Εξουσιοδότηση 17
2.2.2 Ανίχνευση του Συμβάντος 17
2.2.3 Αντιμετώπιση του συμβάντος 18
2.2.4 Συλλογή των ιχνών του δικτύου 18
2.2.5 Προστασία και διατήρηση 19
2.2.6 Διερεύνηση 19
2.2.7 Ανάλυση 20
2.2.8 Διερεύνηση και απόδοση της πηγής της επίθεσης 21
2.2.9 Παρουσίαση και ανασκόπηση 21
2.3 Σενάριο συστηματικής διερεύνησης δικτύων υπολογιστών 22
2.4. Μεθοδολογία ασφαλούς ανάκτησης και ανάλυσης διαδικτυακών δεδομένων 22
2.4.1 Προετοιμασία και Εξουσιοδότηση 24
2.4.2 Αναγνώριση 25
2.4.3 Τεκμηρίωση, Συλλογή, και Διατήρηση 29
2.4.4 Φιλτράρισμα και αφαίρεση δεδομένων 33
2.4.5 Χαρακτηριστικά κλάσης και επιβεβαίωση πηγής 35
2.4.6 Ανάκτηση ψηφιακών αποδεικτικών στοιχείων 40
2.4.7 Αναδημιουργία της διαδικασίας διερεύνησης δικτύων 42
2.5. Διερεύνηση δικτύων στο φυσικό επίπεδο δικτύωσης και επίπεδο ζεύξης 46

2.6. Διερεύνηση δικτύων στο επίπεδο μεταφοράς 50
2.6.1 Αρχεία καταγραφής αυθεντικοποίησης χρήστη 51
2.6.2 Αρχεία καταγραφής εφαρμογών 52
2.6.3 Αρχεία καταγραφής λειτουργικών συστημάτων 53
2.6.4 Αρχεία καταγραφής δικτυακών συσκευών 54
2.6.5 Πίνακες κατάστασης 56
2.6.6 Περιεχόμενα μνήμης RAM 58
3. Τεχνικές συστηματικής διερεύνησης δικτύων υπολογιστών 60
3.1 Παρακολούθηση δικτύου και καταγραφή 60
3.2 Ιχνηλάτιση ηλεκτρονικού ταχυδρομείου 61
3.3 Αναζήτηση των ιχνών της IP προέλευσης 62
3.4 Αναδημιουργία της επίθεσης και των αποδεικτικών στοιχείων 62
3.5 Διχοτόμηση πακέτων 63
3.6 Αναδημιουργία ροής TCP 64
3.7 Ερμηνεία του πρωτοκόλλου HTTP 65
3.8 Κρυφή μνήμη του περιηγητή ιστού 67
3.9 Εφαρμογές Διαδικτύου – Διαδικτυακό ταχυδρομείο 68
3.10 Μέθοδοι καταγραφής της κίνησης δικτύου με τη χρήση υλικού 69
3.10.1 Ομφαλός (Repeater Hub) 69
3.10.2 Μεταγωγείς (Managed Switch) – Διασυνδεδεμένες Θύρες (Spanning Ports) 70
3.10.3 Χρησιμοποιώντας ένα δίκτυο TAP 71
4. Εργαλεία της Δικανικής Δικτύων 72
4.1 Εργαλεία που βασίζονται σε τερματικά συστήματα 73
4.1.1 Ethereal 74
4.1.2 Wireshark 74
4.1.3 TcpDump 74
4.1.4 Xprobe2 75
4.1.5 Snort 76
4.1.6 Argus 76
4.1.7 Netstat 77
4.1.8 Fiddler 77
4.1.9 NTLast 77
4.1.10 p0f 78
4.1.11 Fport 78
4.2 Εργαλεία που βασίζονται σε δίκτυα υπολογιστών 78
4.2.1 Niksun NetDetector 79
4.2.2 Niksun NetIntercept 79
4.2.3 Pcap 80
4.2.4 SiLK 80
4.2.5 Nmap 81
4.2.6 PyFlag 81
4.2.7 Raytheon SilentRunner 82
4.2.8 NetWitness Investigator 82
4.2.9 Bro 83
4.2.10 Ettercap 83
4.2.11 Xplico 83
4.3 Εργαλεία ανάλυσης μηνυμάτων ηλεκτρονικού ταχυδρομείου 84
4.3.1 eMailTrackerPro 85
4.4 Εργαλεία περιηγητών ιστού 85
4.4.1 Mandriant Web Historian 86

4.4.2 Index.dat analyzer 86
5. Εργαστήριο Network Forensics 86
5.1 Απαιτήσεις 87
5.2 Χωροταξία 87
5.3 Εξοπλισμός 88
5.4 Ρυθμίσεις 89
5.4.1 Ρυθμίσεις στα MS Windows 89
5.4.1.1 Ρυθμίσεις του Snort 89
5.4.1.2 Ρυθμίσεις του Nmap 90
5.4.1.3 Ρυθμίσεις του Wireshark 90
5.4.2 Ρυθμίσεις στο Backtrack Linux 90
5.4.2.1 Ρυθμίσεις του Pyflag 91
5.4.2.2 Ρυθμίσεις του xplico 92
6. Σενάρια – Ασκήσεις 94
6.1 Snort 94
6.1.1 Γενικά για το εργαλείο Snort 94
6.1.2 Άσκηση 94
6.2 Pyflag 96
6.2.1 Γενικά για το εργαλείο Pyflag 96
6.2.2 Άσκηση 96
6.3 P0f 98
6.3.1 Γενικά για το εργαλείο P0f 98
6.3.2 Άσκηση 98
6.4 Xprobe2 99
6.4.1 Γενικά για το εργαλείο Xprobe2 99
6.4.2 Άσκηση 99
6.5 Xplico 100
6.5.1 Γενικά για το εργαλείο Xplico 100
6.5.2 Άσκηση 100
7. Συμπεράσματα 102
8. Βιβλιογραφία 103

0. Εισαγωγή

Τα τελευταία χρόνια διαφαίνεται όλο και περισσότερο η ανάγκη για μεγαλύτερη ασφάλεια των συστημάτων ενός οργανισμού από κακόβουλες επιθέσεις εγκληματιών. Πάραυτα σε πολλές περιπτώσεις η επαυξημένη ασφάλεια δεν επαρκεί καθώς οι εγκληματίες εξελίσσουν τις μεθόδους δράσης τους και επιτυγχάνουν καίρια πλήγματα στους οργανισμούς. Αυτό είναι ζήτημα που η ασφάλεια πληροφοριακών συστημάτων δεν μπορεί να απαντήσει και σε αυτό το σημείο καλούνται οι ερευνητές να καταγράψουν, να ερευνήσουν και να αναλύσουν την κίνηση δικτύου ώστε να εξάγουν έγκυρα ψηφιακά αποδεικτικά στοιχεία, να αποδειχθεί η υπαιτιότητα μίας δραστηριότητας και να βρεθεί ο ύποπτος. Αντικείμενο της εργασίας είναι η μελέτη της σχετικής βιβλιογραφίας και η ταξινόμηση των σχετικών τεχνολογιών, μεθόδων, εργαλείων και τεχνικών πραγματοποίησης ερευνών Network Forensics. Στα επιμέρους κεφάλαια της παρακάτω εργασίας δίνουμε το γενικότερο πεδίο της επιστήμης όπου ανήκουν τα Network Forensics. Αναλύεται η επιστήμη των Forensics στους επιμέρους κλάδους της, καθώς και τα πεδία των εφαρμογών τους. Ορίζεται ο κλάδος της ψηφιακής δικανικής όπου ανήκει η δικανική δικτύων. Στη συνέχεια συγκρίνουμε τη δικανική δικτύων και τα συστήματα ανίχνευσης παρείσφρησης ώστε να γίνει κατανοητός ο διαχωρισμός τους. Στο επόμενο κεφάλαιο αναπτύσσεται η μεθοδολογία της ψηφιακής δικανικής ως γενικότερος κλάδος της δικανικής δικτύων και στη συνέχεια παρουσιάζεται και αναλύεται ένα γενικό πλαίσιο της δικανικής δικτύων, καθώς και ένα σενάριο συστηματικής διερεύνησης δικτύων υπολογιστών. Κατόπιν παρουσιάζεται και αναλύεται η μεθοδολογία ασφαλούς ανάκτησης και ανάλυσης δεδομένων στα επιμέρους βήματα της μεθοδολογίας αυτής. Στη συνέχεια αναλύουμε τη διερεύνηση δικτύων σε σχέση με τα επίπεδα δικτύωσης. Ακόμη παρουσιάζουμε όλες τις διαθέσιμες τεχνικές διερεύνησης δικτύων τόσο με τη χρήση λογισμικού όσο και υλικού. Στο επόμενο κεφάλαιο παρουσιάζονται αρκετά εργαλεία τα οποία είναι διαθέσιμα στους ερευνητές δικτύων και διαχωρίζονται ανάλογα με τα συστήματα στα οποία γίνεται η διερεύνηση. Στο επόμενο κεφάλαιο υλοποιείται ένα εργαστήριο Network Forensics στα πλαίσια του Πανεπιστημίου στο οποίο γίνονται κάποιες παραδοχές, και δημιουργούνται κάποιες πρότυπες ασκήσεις για τους χρήστες του εργαστηρίου. Τέλος εξάγονται κάποια χρήσιμα συμπεράσματα που εξήχθησαν από αυτήν την εργασία και μπορούν να γίνουν αντικείμενο περαιτέρω μελέτης.

1. Forensics - Η Επιστήμη των Forensic

Οι έννοιες των forensics και επιστήμης των forensic είναι ταυτόσημες στη διεθνή βιβλιογραφία. Είναι η εφαρμογή ενός ευρέος φάσματος επιστημών που απαντούν σε ερωτήματα τα οποία αφορούν το νομικό σύστημα. Σχετίζεται τόσο με εγκλήματα όσο και με την πολιτική αγωγή. Η επιστήμη των forenscic διαδραματίζει ζωτικό ρόλο στο δικαστικό σύστημα παρέχοντας επιστημονικά αποδεδειγμένες πληροφορίες στους ερευνητές, οι οποίοι αναλύουν τα αποδεικτικά στοιχεία που συνέλεξαν.

Η διερεύνηση των forensics περιλαμβάνει τα παρακάτω βήματα:

- Συλλογή αποδεικτικών στοιχείων από το χώρο του εγκλήματος.
- Ανάλυση των στοιχείων στο εργαστήριο.
- Παρουσίαση των αποτελεσμάτων στο δικαστήριο.

Ανάλογα με το έγκλημα που διερευνάται μπορεί να απαιτούνται η συλλογή, εξέταση και ανάλυση μεγάλου όγκου αποδεικτικών στοιχείων και εξειδικευμένοι επιστήμονες με γνώσεις βιολογίας, χημείας, φυσικής, πληροφορικής και άλλων επιστημών. Αυτοί οι ερευνητές εργάζονται ξεχωριστά για την ανάλυση των αποδεικτικών στοιχείων μίας υπόθεσης και στη συνέχεια συνδυάζονται όλα τα αποτελέσματα των ερευνητών για να συγκροτηθεί η υπόθεση. (http://www.nij.gov).

1.1 Κλάδοι των forensics

1.1.1 Επιστήμες Φυσιολογίας

Σε αυτόν τον κλάδο των forensics ανήκουν οι επιστήμες της ανθρωπολογίας, αρχαιολογίας, οδοντιατρικής, εντομολογίας και παθολογίας.

1.1.1.1 Δικανική Ανθρωπολογία

Ανθρωπολογία είναι η εφαρμογή της κλασσικής ανθρωπολογίας στο νομικό περιβάλλον και χρησιμοποιείται συνηθέστερα στην ανεύρεση και αναγνώριση των ανθρώπινων σκελετών. Η ανθρωπολογία χρησιμοποιείται τις περισσότερες φορές σε ποινικές υποθέσεις όπου τα ανθρώπινα υπολείμματα του θύματος βρίσκονται σε προχωρημένο στάδιο αποσύνθεσης και μπορεί να βοηθήσει στην αναγνώριση αποθανόντων των οποίων τα υπολείμματα έχουν αποσυντεθεί, καεί, ακρωτηριαστεί ή γενικά δεν μπορεί να γίνει η αναγνωριστεί η ταυτότητα του θύματος. Εκτός των παραπάνω η ανθρωπολογία μελετά την ποικιλομορφία, ανάπτυξη, αύξηση και εξέλιξη του ανθρώπινου σκελετού. (Bell S.,2008) Οι ερευνητές του κλάδου, συνήθως εργάζονται σε συνεργασία με παθολόγους, οδοντιάτρους και ερευνητές ανθρωποκτονιών, ώστε να ταυτοποιήσουν το θύμα με κάποιο προγονό του, να ανακαλύψουν αποδεικτικά στοιχεία σε ένα τραύμα και τέλος να καθορίσουν το χρονικό διάστημα από το θάνατο του θύματος.

1.1.1.2 Δικανική Αρχαιολογία

Η αρχαιολογία εφαρμόζεται συνδυάζοντας τεχνικές της αρχαιολογίας και της επιστήμης των forensics. Συχνά η αρχαιολογία θεωρείται μέρος της δικανικής ανθρωπολογίας παρόλα αυτά εξελίσσεται σαν ξεχωριστός αλλά παρεμφερής κλάδος. Γενικά ο τομέας της δικανικής ανθρωπολογίας επικεντρώνεται στην ανάλυση των ανθρώπινων υπολειμμάτων ενώ η δικανική αρχαιολογία επικεντρώνεται στην εύρεση της τοποθεσίας των ανθρώπινων υπολειμμάτων και στην εκσκαφή τους.

Οι αρχαιολόγοι έχουν αναπτύξει λεπτομερείς και συστηματικές μεθόδους εντοπισμού, έρευνας, ανασκαφής και καταγραφής τόπων ενταφιασμού, και χρησιμοποιούν τις πληροφορίες που αποκτήθηκαν για να ανακατασκευάσουν πιθανές δραστηριότητες στην τοποθεσία αυτή. Αυτές οι διαδικασίες προσαρμόζονται ιδανικά για την εξέταση μυστικών τάφων καθώς και για ανάλυση και ανακατασκευή της σκηνής ενός εγκλήματος, ειδικότερα όταν η σκηνή του εγκλήματος δεν έχει ανακαλυφθεί για μεγάλο χρονικό διάστημα.

Περιοχές Εφαρμογών

Οι δικανικοί αρχαιολόγοι συμμετέχουν τόσο στην εύρεση της τοποθεσίας και ανασκαφή των ανθρωπίνων υπολειμμάτων, στην ανάκτηση των ανθρώπινων υπολειμμάτων, εγκληματικών πράξεων, όπλων, κλεμμένων αγαθών, και άλλα ενδεχόμενα αποδεικτικά στοιχεία του εγκλήματος ή του δυστυχήματος. Παράλληλα οι δικανικοί αρχαιολόγοι έχουν αναπτύξει αρχές οι οποίες περιλαμβάνουν την διατήρηση των αντικειμένων, λαμβάνοντας υπόψη τις χημικές και βιολογικές διαδικασίες που διενεργούνται κατά την αποδόμηση των υλικών. Ο δικανικός αρχαιολόγος μελετά και προβλέπει την κατάσταση των υλικών που είναι θαμμένα στο έδαφος, ώστε να εξηγήσει το μοτίβο των αποδεικτικών στοιχείων που βρέθηκαν. Η μελέτη των διαδικασιών αποδόμησης του ανθρώπινου πτώματος, σχετίζεται με την κατάσταση των αντικειμένων και των αποδεικτικών στοιχείων που προέκυψαν από τη διερεύνηση, και βρίσκουν χρησιμότητα στην επιβολή του νόμου ή άλλες αρχές.

1.1.1.3 Δικανική Οδοντιατρική

Η δικανική οδοντιατρική ή δικανική οδοντολογία ορίζεται ως ο σωστός χειρισμός, εξέταση και επαλήθευση των οδοντιατρικών αποδεικτικών στοιχείων, τα οποία στη συνέχεια παρουσιάζονται στη δικαιοσύνη. Τα αποδεικτικά στοιχεία τα οποία εξάγονται από την μελέτη της οδοντοστοιχίας είναι η ηλικία (στην περίπτωση που αφορούν παιδιά) και η αναγνώριση ενός ατόμου στον οποίο ανήκει η οδοντοστοιχία. Αυτό επιτυγχάνεται χρησιμοποιώντας οδοντιατρικές πρακτικές, οι οποίες περιλαμβάνουν, ραδιογράφους, προθανάτιες και επιθανάτιες φωτογραφίες καθώς και το γενετικό υλικό. Οι άλλοι τύποι αποδεικτικών στοιχείων που μελετά αυτός ο κλάδος είναι τα σημάδια από δαγκωματιές, είτε στο θύμα, είτε στον εισβολέα, είτε σε ένα αντικείμενο το οποίο βρέθηκε στη τοποθεσία του εγκλήματος.

Περιοχές Εφαρμογών

- Ταυτοποίηση θυμάτων από τα ανθρώπινα υπολείμματά τους
- Ταυτοποίηση προσώπων σε μαζικούς θανάτους
- Αξιολόγηση των τραυματισμών από δαγκωματιές

- Αξιολόγηση σε περιπτώσεις κακομεταχείρισης
- Πολιτικές υποθέσεις

1.1.1.4 Δικανική Εντομολογία

Η δικανική εντολομολογία αφορά την διερεύνηση των εντόμων που βρίσκονται μέσα πάνω ή γύρω από τα ανθρώπινα απομεινάρια ώστε να καθοριστεί ο χρόνος ή η τοποθεσία θανάτου ή ακόμη και εάν μεταφέρθηκε το θύμα μετά από το θάνατο του.

1.1.1.5 Δικανική Παθολογία

Η δικανική παθολογία είναι το πεδίο της επιστήμης που καθορίζει την αιτία θανάτου ή τραυματισμού, εφαρμόζοντας της αρχές της φαρμακευτικής και της ιατρικής.

Περιοχές Εφαρμογών

Οι δικανικοί παθολόγοι διερευνούν για τραυματισμούς ή αρρώστια που συνδέει άμεσα ή αποτελεί την αφετηρία για μία σειρά από γεγονότα τα οποία οδηγούν στο θάνατο ενός ατόμου. Ακόμη καθορίζουν την κύρια αιτία θανάτου, η οποία στις περισσότερες περιπτώσεις είναι είτε ανθρωποκτονία, είτε τυχαία, είτε φυσική, είτε αυτοκτονία, είτε απροσδιόριστη. Ακόμη μπορεί να γίνει συλλογή αποδεικτικών στοιχείων ή να καθοριστεί η ταυτότητα του αποθανόντος. Επίσης εξετάζονται και καταγράφονται οι πληγές και οι τραυματισμοί. Γίνεται τοξικολογική ανάλυση στους ιστούς και τα υγρά του σώματος, για να καθοριστεί εάν υπήρχε, για παράδειγμα, σκόπιμη δηλητηρίαση.

1.1.2 Κοινωνικές Επιστήμες

Σε αυτόν τον κλάδο των forensics ανήκουν οι επιστήμες της ψυχολογίας και ψυχιατρικής.

1.1.2.1 Δικανική Ψυχολογία και Ψυχιατρική.

Η δικανική ψυχολογία είναι η μελέτη της ψυχολογίας ενός ατόμου, χρησιμοποιώντας τεχνικές των forensics. Με αυτόν τον τρόπο καθορίζονται συνήθως οι συνθήκες πίσω από μία εγκληματική συμπεριφορά. Οι κλάδοι της ψυχολογίας και ψυχιατρικής είναι αλληλένδετοι στη βιβλιογραφία. Οι Βοηθούν τους ψυχολόγους και ψυχιάτρους στην κατανόηση του ποινικού νόμου, ώστε να είναι ικανοί να επικοινωνήσουν σωστά με δικαστές, δικηγόρους και άλλους επαγγελματίες νομικούς. Μία σημαντική πλευρά της δικανικής ψυχολογίας και ψυχιατρικής είναι η ικανότητα κατάθεσης στο δικαστήριο, αναδιατυπώνοντας τα ψυχολογικά ευρήματα στη νομική γλώσσα του δικαστηρίου, παρέχοντας πληροφορίες στο νομικό προσωπικό με κατανοητό τρόπο. Με τη βοήθεια αυτών των επιστημών αποκτούμε συμπεριφορικά αποδεικτικά στοιχεία τα οποία είναι αόριστα και υπόκεινται σε διαφορετικές οπτικές γωνίες και ερμηνείες.

Περιοχές Εφαρμογών

Περιλαμβάνουν τον καθορισμό της εγκληματικής ευθύνης και την εγκυρότητα του ισχυρισμού φρενοβλάβειας ή όχι, αξιολογώντας την επικινδυνότητα του ατόμου για την κοινωνία και την πιθανότητα να παραβεί τον νόμο. Αξιολογούν τόσο τα θύματα όσο και τους παραβάτες, μελετούν την επιθετική συμπεριφορά, και επαληθεύουν την κατάθεση του αυτόπτη μάρτυρα.

1.1.3 Εγκληματολογία

Σε αυτόν τον κλάδο των forensics ανήκουν οι επιστήμες της βαλλιστικής, γενετικής, δακτυλοσκοπίας, ποδιατρικής και τοξικολογίας.

1.1.3.1 Βαλλιστική

Είναι η μελέτη των μηχανισμών που ασχολούνται με την πτήση, τη συμπεριφορά και την επίδραση των βλημάτων, ειδικότερα των σφαιρών, των βομβών βαρύτητας, των πυραύλων ή ομοειδών βλημάτων. Αποτελεί την επιστήμη ή την τέχνη του σχεδιασμού και επιτάχυνσης των βλημάτων έτσι

ώστε να επιτευχθεί η επιθυμητή επίδοση. Μία σημαντική υποκατηγορία της βαλλιστικής είναι η μελέτη των βαλλιστικών αποτυπωμάτων η οποία αναφέρεται σε ένα σύνολο δικανικών τεχνικών οι οποίες στηρίζονται σε σημάδια που αφήνουν τα όπλα σε σφαίρες, ώστε να αντιστοιχιστεί μία σφαίρα με ένα όπλο από το οποίο πυροβολήθηκε, εκτελώντας αναζητήσεις σε μεγάλες βάσεις δεδομένων.

Περιοχές Εφαρμογών

Οι βάσεις δεδομένων, που χρησιμοποιούνται για τα βαλλιστικά αποτυπώματα, περιλαμβάνουν εικόνες και εγγραφές από όλα τα νέα όπλα που πωλούνται, οι οποίες αυξάνουν σημαντικά τον όγκο και το πεδίο δράσης αυτών των βάσεων δεδομένων.

1.1.3.2 Γενετική

Είναι η τεχνική που χρησιμοποιείται από επιστήμονες ώστε να βοηθήσει στην αναγνώριση υπόπτων από τα αντίστοιχα προφίλ DNA. Τα προφίλ DNA είναι κρυπτογραφημένα σύνολα αριθμών τα οποία αντικατοπτρίζουν το DNA ενός ατόμου, και μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του ατόμου.

1.1.3.3 Δακτυλοσκοπία

Η αναγνώριση δακτυλικών αποτυπωμάτων ή αλλιώς δακτυλοσκοπία, είναι η διαδικασία της σύγκρισης δύο αποτυπωμάτων, από τα ανθρώπινα δάκτυλα ή από την παλάμη του χεριού, ώστε να καθοριστεί εάν αυτά τα αποτυπώματα προέρχονται από το ίδιο πρόσωπο.

Περιοχές Εφαρμογών

Τα αποδεικτικά στοιχεία από την δακτυλοσκοπία μπορούν να συλλεχθούν, να διατηρηθούν και να διανεμηθούν με διαφορετικούς τρόπους. Η επιλογή που θα κάνουμε εξαρτάται από τις επικρατούσες συνθήκες. Όταν βρεθούν στη τοποθεσία του εγκλήματος αντικείμενα όπως όπλα ή χαρτί και πρέπει να πάρουμε αποτυπώματα από αυτά, το αντικείμενο στο οποίο βρέθηκαν τα αποτυπώματα στέλνετε

στον αναλυτή αποτυπωμάτων, αντί να αναπτυχθεί στο πεδίο του εγκλήματος. Επίσης, αποτυπώματα τα οποία βρίσκονται επάνω σε αφαιρούμενες επιφάνειες αποκόπτονται και στέλνονται στον αναλυτή αποτυπωμάτων. Όπως και με όλα τα αποδεικτικά στοιχεία, σε κάθε περίπτωση είναι απαραίτητη η πλήρης και αναλυτική καταγραφή φωτογραφίζοντας τα αποδεικτικά στοιχεία, ειδικότερα σε περιπτώσεις όπου είναι απίθανο ότι τα αποτυπώματα μπορούν να αναπαραχθούν ή να μεταφερθούν από το σημείο στο οποίο βρέθηκαν.

1.1.3.4 Ποδιατρική

Η ποδιατρική είναι η εφαρμογή της μελέτης των αποτυπωμάτων ενός πέλματος ή ενός υποδήματος και των ιχνών που άφησαν στην τοποθεσία του εγκλήματος ώστε να αποδειχθεί κατά τη διερεύνηση η ταυτότητα ενός προσώπου. Τα αποδεικτικά στοιχεία από τα αποτυπώματα ενός παπουτσιού βρίθουν σε αφθονία στην τοποθεσία ενός εγκλήματος και στις περισσότερες περιπτώσεις μπορούν να αποδειχθούν ίσης αξίας με τα δακτυλικά αποτυπώματα.

Περιοχές Εφαρμογών

Αρχικά οι ερευνητές προσπαθούν να αναγνωρίσουν τον κατασκευαστή και το μοντέλο του υποδήματος από το οποίο προήλθε το αποτύπωμα. Αυτό μπορεί να γίνει είτε οπτικά είτε συγκρίνοντάς το με μία βάση δεδομένων. Η επιτυχία αυτών των μεθόδων εξαρτάται από την αναγνώριση του μοτίβου, τα σημάδια της μάρκας και του λογότυπου. Μπορούν να εξαχθούν πληροφορίες σχετικά με τον ιδιοκτήτη του υποδήματος οι οποίες εξαρτώνται από την γωνία της πατημασιάς και την κατανομή του βάρους. Η λεπτομερής ανάλυση των αποτυπωμάτων ενός υποδήματος, μπορούν να βοηθήσουν στη σύνδεση ενός συγκεκριμένου υποδήματος με το αποτύπωμά του, καθώς κάθε υπόδημα έχει μοναδικά χαρακτηριστικά.

1.1.3.5 Τοξικολογία

Είναι η μελέτη της ανίχνευσης και αναγνώρισης για παράνομες ναρκωτικές ουσίες, χημικούς καταλύτες οι οποίοι χρησιμοποιούνται σε περιπτώσεις εμπρησμών, εκρηκτικών μηχανισμών και

πυροβολισμών. Η κύρια μέριμνα του ερευνητή δεν είναι το νομικό αποτέλεσμα από την διερεύνηση ή η τεχνολογία που χρησιμοποιήθηκε, αλλά η σωστή εξαγωγή και ερμηνεία των αποτελεσμάτων.

Περιοχές Εφαρμογών

Ένας τοξικολόγος πρέπει να λάβει υπόψη του το περιεχόμενο μίας διερεύνησης, και συγκεκριμένα κάθε φυσικό σύμπτωμα το οποίο έχει καταγραφεί, κάθε αποδεικτικό στοιχείο που έχει συλλεχθεί από τη σκηνή ενός εγκλήματος και μπορεί να περιορίσει την αναζήτηση, όπως μπουκάλια με χάπια, σκόνες, επαλείμματα ιχνών, καθώς και άλλες διαθέσιμες χημικές ουσίες. Βάσει αυτών των πληροφοριών και των δειγμάτων, οι τοξικολόγοι καθορίζουν την παρουσία τοξικών ουσιών, τις συγκεντρώσεις τους, καθώς και τις πιθανές επιπτώσεις αυτών των χημικών στον ανθρώπινο οργανισμό.

1.1.4 Ψηφιακή Δικανική

Η ψηφιακή δικανική είναι ένας κλάδος της επιστήμης των forensics η οποία περιλαμβάνει την ανάκτηση και διερεύνηση υλικού σε ψηφιακές συσκευές και συχνά σχετίζεται με το ηλεκτρονικό έγκλημα. Ο όρος της ψηφιακής δικανικής (digital forensics) αρχικά χρησιμοποιήθηκε ως συνώνυμο του όρου της δικανικής υπολογιστών (computer forensics) αλλά επεκτάθηκε ο ορισμός του καλύπτοντας όλες τις συσκευές οι οποίες είναι ικανές να αποθηκεύσουν ψηφιακά δεδομένα, περιλαμβάνοντας κινητές συσκευές, βάσεις δεδομένων και δίκτυα, και αυτή τη στιγμή ο όρος μπορεί να χρησιμοποιηθεί ώστε να περιγράψει το σύνολο του κλάδου. Το 2001 στο πρώτο Digital Forensic Research Workshop αναγνωρίστηκε η ανάγκη να αναθεωρηθεί ο όρος και προτάθηκε ο όρος digital forensic science για να περιγράψει το πεδίο της επιστήμης. Επίσης χρησιμοποιούνται ευρύτητα οι όροι forensic computer analysis και forensic computing. (Casey et al, 2004)

Περιοχές Εφαρμογών

Οι διερευνήσεις που πραγματοποιούνται στα πλαίσια της ψηφιακής δικανικής ποικίλουν, και τυπικά περιλαμβάνουν αποδεικτικά στοιχεία που ανακτήθηκαν από υπολογιστικά συστήματα, από το διαδίκτυο, ή από διερευνήσεις εισβολών σε δίκτυα. Ο κλάδος αυτός μπορεί να χρησιμοποιηθεί για

να αναγνωρισθεί ένα έγκλημα, να αναγνωρισθούν ύποπτοι, να επαληθευτεί το αληθές των δηλώσεων αλλά ακόμη και να αποδειχθεί η αυθεντικότητα εγγράφων.

Η ψηφιακή δικανική αποτελεί το μεγαλύτερο και πιο πολύπλοκο κομμάτι της δικανικής επιστήμης. Οι κλάδοι που ανήκουν στην ψηφιακή δικανική είναι η δικανική υπολογιστών, η δικανική κινητών συσκευών και η δικανική δικτύων.

1.1.4.1 Δικανική Υπολογιστών

Επικρατεί σύγχυση ως προς τον ορισμό της δικανικής υπολογιστών (computer forensics) στη διεθνή βιβλιογραφία μιας και σημαίνει διαφορετικά πράγματα σε διαφορετικούς ανθρώπους. Ένας απλός ορισμός της δικανικής υπολογιστών είναι η διαδικασία της εφαρμογής επιστημονικών και αναλυτικών τεχνικών στα λειτουργικά συστήματα των υπολογιστών και των δομών των αρχείων με αποτέλεσμα τη δημιουργία νομικά αποδεδειγμένων αποδεικτικών στοιχείων. Επίσης ο όρος δικανική υπολογιστών υιοθετήθηκε από την κοινότητα της ασφάλειας πληροφοριών για να περιγράψει ένα μεγάλο εύρος εργασιών που έχουν να κάνουν περισσότερο με την προστασία των υπολογιστικών συστημάτων παρά με τη συλλογή αποδεικτικών στοιχείων. (Casey et al,2004)

Περιοχές Εφαρμογών

Η δικανική υπολογιστών συνήθως αναφέρεται στις τεχνικές ανάλυσης των υποσυστημάτων και των περιεχομένων ενός υπολογιστή, όπως σκληροί δίσκοι, ψηφιακοί δίσκοι και εκτυπωτές. Ο στόχος της δικανικής υπολογιστών είναι η εξέταση των ψηφιακών μέσων με δικανικές μεθόδους με σκοπό την αναγνώριση, διατήρηση, ανάκτηση, ανάλυση και παρουσίαση των γεγονότων και απόψεων σχετικά με την πληροφορία που αποκτήθηκε.

1.1.4.2 Δικανική Κινητών Συσκευών

Η δικανική κινητών συσκευών είναι ο κλάδος των δικανικών επιστημών που περιλαμβάνει την ανάκτηση ψηφιακών αποδεικτικών στοιχείων από μία κινητή συσκευή υπό το πρίσμα των forensics

χρησιμοποιώντας επιστημονικά αποδεδειγμένες μεθόδους. (Jansen W., 2007)

Οι κινητές συσκευές μπορεί να περιλαμβάνουν χρήσιμα δεδομένα και με τη βοήθεια της δικανικής κινητών συσκευών είμαστε ικανοί να εξάγουμε όλα αυτά τα δεδομένα αποκτώντας χρήσιμη πληροφορία. Ωστόσο ανακύπτουν δύο θέματα. Τα κινητά τηλέφωνα παρουσιάζουν πολλά εμπόδια στον ερευνητή, περιλαμβάνοντας την ποικιλομορφία των λειτουργικών συστημάτων που χρησιμοποιούνται και πολλούς παρόχους κινητής δικτύωσης. Συνδυαζόμενα αυτά τα θέματα παράγουν άγνωστα συστήματα αρχείων, διαφορετικό υλικό, διαφορετικά καλώδια και φορτιστές. Οι διερευνητές θα πρέπει να είναι σε θέση να μάθουν όλες τις ενδεχόμενες πηγές αποδεικτικών στοιχείων τα οποία μπορεί να βρεθούν σε κινητά τηλέφωνα, καθώς και να γίνουν κύριοι των διαθέσιμων επιλογών για αξιόπιστη συλλογή από τις συσκευές και τις διαθέσιμες μεθόδους ώστε να εντοπίσουν τα χρήσιμα αποδεικτικά στοιχεία. (2008)

Περιοχές Εφαρμογών

Η δικανική κινητών συσκευών διαφοροποιείται σε σχέση με τη δικανική υπολογιστών λόγω των διαφορετικών χαρακτηριστικών των κινητών συσκευών σε σχέση με τους παραδοσιακούς υπολογιστές. Περιλαμβάνει την ανάλυση των υποσυστημάτων μίας κινητής συσκευής, όπως την κάρτα SIM, την εσωτερική μνήμη και εξωτερική μνήμη.

1.1.4.3 Δικανική Δικτύων

Τα network forensics αναφέρονται στα αποδεικτικά στοιχεία όπως αρχεία καταγραφής που διατηρούνται από παρόχους υπηρεσιών διαδικτύου, και από άλλους απομακρυσμένους δικτυωμένους υπολογιστές. Τα network forensics σχετίζονται περισσότερο με την έρευνα των απομακρυσμένων επιθέσεων, όπως απομακρυσμένες επιθέσεις άρνησης εξυπηρέτησης. (Caloyannides, 2004)

Τα network forensics ορίζονται ως η διαδικασία ανάκτησης και ανάλυσης πληροφοριών από ένα ή περισσότερα δίκτυα υπολογιστών, για τα οποία υποψιαζόμαστε ότι εκτέθηκαν ή προσπελάστηκαν από μη εξουσιοδοτημένους χρήστες. Οι πληροφορίες αυτές περιλαμβάνουν την κίνηση του δικτύου

και τα φορτία δεδομένων. Τα network forensics επιτρέπουν στους αναλυτές να επεξεργαστούν την εγκυρότητα των υποθέσεων προσπαθώντας να εξηγήσουν τις συνθήκες και τα αίτια της ενέργειας που ερευνούν, και αν είναι δυνατόν να παρέχουν αποδεικτικά στοιχεία που θα υποστηρίξουν είτε ποινική είτε αστική ευθύνη. (Mohay et al, 2003)

Ο ορισμός που δόθηκε για τα network forensics στο πρώτο Digital Forensic Research Workshop, το 2001 είναι ο εξής:

Η χρήση επιστημονικά αποδεδειγμένων τεχνικών για την συλλογή, αναγνώριση, εξέταση, συσχέτιση, ανάλυση και καταγραφή των ψηφιακών αποδεικτικών στοιχείων από πολλαπλές, ενεργές ψηφιακές πηγές, επεξεργασίας και μετάδοσης, για τον σκοπό της αποκάλυψης γεγονότων σχετικών με την προσχεδιασμένη πρόθεση, ή τη μετρήσιμη επιτυχία των μη εξουσιοδοτημένων ενεργειών που έχουν ως σκοπό την διατάραξη, φθορά, ή και τον κίνδυνο των συστατικών του συστήματος, καθώς και την παροχή πληροφοριών ώστε να βοηθήσει στην απάντηση ή την επαναφορά από αυτές τις ενέργειες.

Με την ανάπτυξη του διαδικτύου, οι επιθέσεις μέσω διαδικτύου και οι παραβιάσεις της ασφάλειας έχουν αυξηθεί. Οι υπάρχουσες μέθοδοι όπως η εξέταση των αρχείων ιστορικού που διατηρούνται στους διακομιστές, οι εγγραφές των firewall, τα γεγονότα ανίχνευσης παρείσφρησης, τα απολεσθέντα πακέτα, και ούτω καθεξής, δεν επαρκούν για να αναγνωρίσουν τον εξελιγμένο επιτιθέμενο ο οποίος χρησιμοποιεί εργαλεία όπως για παράδειγμα κρυπτογραφία. Τα εργαλεία των network forensics χρησιμοποιούν εξειδικευμένες τεχνικές με δυνατότητες καταγραφής και συσχέτισης δεδομένων από πολλαπλές οντότητες του δικτύου. (Kanellis, 2006).

Τα network forensics είναι η αρχή της αναδημιουργίας των ενεργειών που οδήγησαν σε ένα συμβάν που επιδέχεται περαιτέρω διερεύνησης και δίνουν απάντηση σε ερωτήματα όπως "Τι έκαναν;" αλλά και "Πως το έκαναν;" (Brown, 2006). Ανάλογα με τον τύπο της διερεύνησης μπορεί να ενδιαφερόμαστε για διαφορετικά γεγονότα και να χρησιμοποιήσουμε διαφορετικές πηγές αποδεικτικών στοιχείων. Ωστόσο, ενδιαφερόμαστε συνήθως για πληροφορίες υψηλού επιπέδου σχετικά με διαφορετικές οντότητες και την αλληλεπίδραση μεταξύ τους. Για παράδειγμα, μπορεί να μας ενδιαφέρουν μηνύματα ηλεκτρονικού ταχυδρομείου που εστάλησαν από ένα συγκεκριμένο χρήστη, οι ιστοσελίδες που προσπελάστηκαν ή τα μηνύματα chat που δέχθηκαν (Li, 2010). Η

δικτυακή κίνηση αποτελεί μία εξαιρετική πηγή αποδεικτικών στοιχείων για την διερεύνηση δικτύων, δεδομένου ότι είναι το πρωταρχικό μέσο για την εκτέλεση αλληλεπιδράσεων υψηλού επιπέδου (Casey, 2004). Για παράδειγμα, η αναζήτηση όρων και πρότυπα προσπέλασης του διαδικτύου αποτελούν γενικά καλές ενδείξεις των προθέσεων και του γνωστικού επιπέδου ενός ατόμου.

Συνήθως τα network forensics αποτελούν το αρχικό στάδιο μίας διερεύνησης όταν τα disk forensics δεν μπορούν να ανακτηθούν. Η διαδικασία αυτή μπορεί να εκτελεστεί παθητικά χωρίς την ανάγκη επαγρύπνησης του υπόπτου και μπορεί να είναι ένα σημαντικό μέρος της ανάπτυξης του πεδίου δράσης της διερεύνησης (Li, 2010).

Περιοχές εφαρμογών

Στη διερεύνηση δικτύων αντί να γίνει αντιστοίχιση των παρατηρούμενων δραστηριοτήτων σε ένα τοπικό δίκτυο, με μία βάση δεδομένων από γνωστά πρότυπα κακόβουλων ενεργειών, γίνεται καταγραφή όλων των δραστηριοτήτων στο τοπικό δίκτυο και παρέχονται ολοκληρωμένα εργαλεία για την ανάλυση των δραστηριοτήτων σε πραγματικό χρόνο αλλά και για να εκτιμηθεί η ζημιά από αυτές τις ενέργειες. Αναλόγως της δικτυακής του θέσης το σύστημα μπορεί να παραμείνει απόρθητο σε πιθανή καταστρατήγηση του (Brown, 2006).

1.1.5 Σύγκριση της Δικανικής Δικτύων και των Συστημάτων Ανίχνευσης Παρείσφρησης

Το πεδίο της δικανικής δικτύων φέρει ομοιότητες με τα παραδοσιακά συστήματα ανίχνευσης παρείσφρησης (NIDS). Σε πολλές περιπτώσεις τα NDIS και τα network forensics φαίνονται πανομοιότυπα, καθώς και τα δύο συλλέγουν και αναλύουν την δικτυακή κίνηση. Ωστόσο τα συνηθισμένα NIDS αναπτύχθηκαν με διαφορετικούς στόχους.

Ένα NDIS είναι σχεδιασμένο με γνώμονα την ανίχνευση εισβολών ή παραβίαση την πολιτικής ασφάλειας. Στον αντίποδα το network forensics τυπικά ενδιαφέροντα για την κίνηση η οποία δεν παρουσιάζει κάποια ανωμαλία, και συμμορφώνεται με την πολιτική ασφάλειας. Για παράδειγμα, μηνύματα ηλεκτρονικού ταχυδρομείου ή η δραστηριότητα προσπέλασης του διαδικτύου μπορεί να

ενδιαφέρουν έναν ερευνητή των network forensics, αλλά από την σκοπιά των NDIS θα κατηγοριοποιούνταν ως φυσιολογικά.

Τα NDIS τυπικά καλύπτουν μεγαλύτερα κομμάτια του δικτύου. Συνήθως το σημείο παρεμβολής σε ένα εταιρικό περιβάλλον γίνεται σε ένα σημείο συγκέντρωσης της κίνησης του δικτύου, όπως μία πύλη εισόδου ή σε ένα μεγάλο σύνδεσμο με τα υπόλοιπα υποδίκτυα. Επομένως παρέχεται μεγαλύτερη κάλυψη των συστημάτων και επιτρέπει στα NDIS να παρακολουθούν πολλά συστήματα ταυτόχρονα. Με αυτό τον τρόπο παρέχεται καλύτερη κάλυψη των συστημάτων και επιτρέπει στα NIDS να παρακολουθούν πολλά συστήματα ταυτόχρονα. Εξαιτίας αυτής της συγκεντρωτικής λειτουργίας, τα NDIS τυπικά δεν αποθηκεύουν τα παρεμβαλλόμενα δεδομένα, και όλη η ανάλυση γίνεται σε πραγματικό χρόνο. Από την άλλη πλευρά, τα network forensics χρειάζονται συχνά να λάβουν υπόψη δεδομένα του παρελθόντος. Εξαιτίας αυτής της απαίτησης αλλά και την απαίτηση για αποδεικτικά στοιχεία, τα network forensics σχεδόν πάντα απαιτούν ένα πλήρες αντίγραφο της δικτυακής κίνησης (Li, 2010).

1.1.6 Άλλοι κλάδοι των forensics που δεν εμπίπτουν στις παραπάνω κατηγορίες

- Γεωλογία: Αφορά την ανίχνευση αποδεικτικών στοιχείων στο χώμα, στα άλατα και τα πετρελαιοειδή
- Μετεωρολογία: Είναι η ανάλυση παρελθόντων καιρικών συνθηκών για μία συγκεκριμένη τοποθεσία λόγω απώλειας άλλων πληροφοριών.
- Βοτανολογία: Είναι η μελέτη της ζωής των φυτών ούτως ώστε να αποκτηθούν πληροφορίες αναφορικά με πιθανά εγκλήματα.
- Υπολογιστική: Ασχολείται με την ανάπτυξη αλγορίθμων και λογισμικού για να βοηθήσει τη διαδικασία διερεύνησης,
- Γεωφυσική: Είναι η εφαρμογή γεωφυσικών τεχνικών όπως η ανίχνευση αντικειμένων που είναι κρυμμένα υπόγεια ή κάτω από το νερό.
- Λιμνολογία: Είναι η ανάλυση των αποδεικτικών στοιχείων που συλλέχθηκαν από τον τόπο του εγκλήματος μέσα ή κοντά σε πηγές φρέσκου νερού. Η εξέταση των βιολογικών οργανισμών, μπορεί να χρησιμεύσει για τη σύνδεση υπόπτων με τα θύματα.
- Γλωσσολογία: Ασχολείται με θέματα που άπτονται του νομικού συστήματος και απαιτούν

εξειδικευμένο γλωσσολόγο.

- Οπτομετρία: Είναι η μελέτη των οπτικών ειδών όπως γυαλιά οράσεως, τα οποία σχετίζονται με τη σκηνή ενός εγκλήματος ή και την διερεύνηση εγκλημάτων.
- Σεισμολογία: Είναι η μελέτη τεχνικών που χρησιμοποιούνται για να διαχωρίσουν τα σεισμικά σήματα που δημιουργούνται από υπόγειες πυρηνικές εκρήξεις σε σχέση με τα σήματα που δημιουργούνται από τους σεισμούς.
- Ορρολογία: Είναι η μελέτη των υγρών του σώματος.
- Ανάλυση βίντεο: Είναι η επιστημονική εξέταση, σύγκριση και αξιολόγηση ενός βίντεο υπό νομικούς όρους.
- Ανάλυση των αποδεικτικών στοιχείων: Είναι η ανάλυση και σύγκριση των αποδεικτικών στοιχείων που προκύπτουν από ίχνη όπως γυαλιά, χρώματα, κλωστές και τρίχες.

2. Μεθοδολογία

2.1 Μεθοδολογία της Ψηφιακής Δικανικής

Η βασική μεθοδολογία της ψηφιακής δικανικής αποτελείται από τα έξης στοιχεία:

- Απόκτηση των αποδεικτικών στοιχείων χωρίς την καταστροφή των αυθεντικών στοιχείων
- Πιστοποίηση ότι τα αποκτηθέντα στοιχεία είναι τα ίδια με τα αυθεντικά στοιχεία
- Ανάλυση των δεδομένων χωρίς αυτά να τροποποιηθούν

2.1.1 Απόκτηση των στοιχείων

Θα πρέπει να λάβουμε υπόψη ότι κάθε περίπτωση είναι διαφορετική. Δεν πρέπει να αποσυνδέουμε τους υπολογιστές ή άλλες συσκευές και μέσα, γιατί τα αποδεικτικά στοιχεία μπορεί να βρίσκονται μόνο στη προσωρινή μνήμη. Επομένως η συλλογή των αποδεικτικών στοιχείων θα πρέπει να γίνει

από συστήματα τα οποία είναι σε λειτουργία.

Εφίσταται η προσοχή σε δύο σημεία κλειδιά:

- Χρειάζεται σωστός χειρισμός των αποδεικτικών στοιχείων καθώς σε περίπτωση λάθος χειρισμού όλη η διαδικασία της διερεύνησης θα υπομονευτεί.
- Η Αλυσίδα φύλαξης (Chain of custody): Ο στόχος της διατήρησης μιας καλής αλυσίδας φύλαξης είναι η εξασφάλιση της ακεραιότητας των αποδεικτικών στοιχείων και η αποτροπή της αλλοίωσης τους. Η αλυσίδα πρέπει να απαντά στα εξής ερωτήματα:
    1. Ποιος τα συνέλλεξε
    2. Πως και που
    3. Ποιος τα κατείχε
    4. Πως αποθηκεύθηκαν και πως προστατεύθηκαν κατά την αποθήκευσή τους
    5. Ποιος τα εξήγαγε από την αποθήκευση και γιατί

2.1.2 Αλυσίδα Φύλαξης

Η αλυσίδα φύλαξης περιλαμβάνει τα εξής βήματα:

- Συλλογή: Το ζητούμενο είναι τα αποδεικτικά στοιχεία να είναι αρκετά ξεκάθαρα ώστε να υποστηρίξουν την υπόθεση
- Ταυτοποίηση: Τα αποδεικτικά στοιχεία ταυτοποιούνται μεθοδικά και τοποθετείται ετικέτα σε κάθε στοιχείο που εξάγεται από την τοποθεσία του θύματος ή του υπόπτου
- Μεταφορά: Τα αποδεικτικά στοιχεία δεν πρέπει να μετακινούνται και στην περίπτωση που κρίνεται απαραίτητη η μεταφορά τους θα πρέπει να γίνεται με εξαιρετική προσοχή
- Αποθήκευση: Τα αποθηκευτικά στοιχεία διατηρούνται σε δροσερό και ξηρό σημείο το οποίο είναι κατάλληλο για ηλεκτρονικά πειστήρια
- Τεκμηρίωση της διερεύνησης: Αποτελεί το πιο δύσκολο κομμάτι της διαδικασίας και γίνεται λεπτομερέστατη καταγραφή των διαδικασιών που ακολουθήθηκαν κατά τη διερεύνηση
- Πιστοποίηση της αυθεντικότητας των αποδεικτικών στοιχείων: Κρίνεται δύσκολο βήμα για την όλη διαδικασία καθώς η τοποθεσία του εγκλήματος μεταβάλλεται με την πάροδο του

χρόνου, τα αποδεικτικά στοιχεία συχνά καταστρέφονται από τις περιβαλλοντικές συνθήκες και οι ηλεκτρονικές συσκευές καταστρέφονται με την πάροδο του χρόνου. Διατηρούνται αποδεικτικά στοιχεία της ακεραιότητας των δεδομένων μέσω της κρυπτογράφησης των αρχείων

- Ανάλυση: Διατηρούνται αντίγραφα ασφαλείας των δεδομένων και χρησιμοποιούνται όλα τα γνωστά εργαλεία για να γίνει ανάλυση των αποδεικτικών στοιχείων

2.2 Ένα γενικό πλαίσιο για τη Δικανική Δικτύων

2.2.1 Προετοιμασία και Εξουσιοδότηση

Η δικανική δικτύων εφαρμόζεται μόνο σε περιβάλλοντα όπου υλοποιούνται εργαλεία ασφάλειας δικτύου, όπως συστήματα ανίχνευσης παρείσφρησης, αναλυτές πακέτων, τείχη προστασίας, λογισμικό μέτρησης της ροής της κίνησης δικτύου, σε διάφορα στρατηγικά σημεία στο δίκτυο. Το προσωπικό που χειρίζεται αυτά τα εργαλεία θα πρέπει να έχει εκπαιδευτεί για να εξασφαλιστεί ότι θα συλλεχθούν τα περισσότερα και ποιοτικότερα αποδεικτικά στοιχεία ώστε να διευκολυνθεί η απόδοση ευθυνών στο έγκλημα. Αποκτούνται οι απαιτούμενες εξουσιοδοτήσεις για να παρακολουθηθεί η δικτυακή κίνηση και τίθεται σε εφαρμογή μία καλά καθορισμένη πολιτική ασφάλειας, ώστε να μην παραβιαστεί η ιδιωτικότητα των ατόμων που εργάζονται για τον οργανισμό. Τα Honeynet και τα τηλεσκόπια δικτύου, μπορούν να τοποθετηθούν ώστε να δελεάσουν τους επιτιθέμενους, να μελετήσουν την συμπεριφορά τους και να μάθουν τη στρατηγική τους.

2.2.2 Ανίχνευση του Συμβάντος

Παρακολουθούνται οι προειδοποιήσεις που παράγονται από διάφορα εργαλεία ασφάλειας και υποδεικνύουν μία παραβίαση ασφάλειας ή πολιτικής. Κάθε μη εξουσιοδοτημένο γεγονός και ανωμαλία που παρατηρείται θα αναλυθεί. Η παρουσία και η φύση της επίθεσης καθορίζονται από ποικίλες παραμέτρους. Πραγματοποιείται μία γρήγορη επικύρωση για να εκτιμηθεί και να

επιβεβαιωθεί η επίθεση. Αυτά τα γεγονότα θα διευκολύνουν τη σημαντική απόφαση εάν θα συνεχιστεί η διερεύνηση ή θα αγνοηθεί η προειδοποίηση σαν εσφαλμένος συναγερμός. Θα πρέπει να προνοήσουμε ώστε τα αποδεικτικά στοιχεία να μην μεταβληθούν κατά τη διαδικασία. Η επιβεβαίωση ενός συμβάντος μας οδηγεί σε δύο κατευθύνσεις, να αντιμετωπιστεί ένα συμβάν ή να γίνει συλλογή δεδομένων.

2.2.3 Αντιμετώπιση του συμβάντος

Η αντιμετώπιση ενός εγκλήματος ή μία εξακριβωμένη εισβολή αρχικοποιείται βάσει της πληροφορίας που συλλέχθηκε ώστε να επικυρωθεί και να εκτιμηθεί το συμβάν. Η αρχικοποίηση της αντιμετώπισης του συμβάντος εξαρτάται από τον τύπο της επίθεσης που αναγνωρίστηκε και καθορίζεται από την πολιτική του οργανισμού και το νόμο. Ένα σχέδιο δράσης αρχικοποιείται ώστε να περιοριστούν οι μελλοντικές επιθέσεις και να γίνει ανάκτηση από την υφιστάμενη φθορά. Την ίδια στιγμή λαμβάνεται η απόφαση εάν θα συνεχιστεί η διερεύνηση και θα συλλεχθούν περισσότερες πληροφορίες. Αυτή η φάση εφαρμόζεται μόνο σε περιπτώσεις όπου η διερεύνηση αρχικοποιείται καθώς η επίθεση διενεργείται την ίδια στιγμή.

2.2.4 Συλλογή των ιχνών του δικτύου

Τα δεδομένα αποκτώνται από τους αισθητήρες οι οποίοι χρησιμοποιούνται για να συλλέξουν τα δεδομένα από την κίνηση του δικτύου. Οι αισθητήρες θα πρέπει να είναι ασφαλείς, να έχουν ανοχές σε σφάλματα, να επιτρέπουν περιορισμένη πρόσβαση και θα πρέπει να μην διακινδυνεύσουν από επιθέσεις. Θα πρέπει να πραγματοποιηθεί μία καλά καθορισμένη διαδικασία χρησιμοποιώντας αξιόπιστα εργαλεία, υλικό και λογισμικό ώστε να συλλεχθούν τα περισσότερα πειστήρια προκαλώντας τη μικρότερη δυνατή επίπτωση στο θύμα. Το δίκτυο θα πρέπει να παρακολουθείται ώστε να ανιχνεύσει μελλοντικές επιθέσεις. Η ακεραιότητα των δεδομένων και τα γεγονότα δικτύου που καταγράφονται πρέπει να εξασφαλιστούν. Η συλλογή είναι το πιο δύσκολο σημείο καθώς οι αλλαγές στα δεδομένα δικτύου γίνονται με ταχείς ρυθμούς και δεν είναι δυνατό να βρεθούν τα ίδια

πειστήρια σε μελλοντικό χρόνο. Το ποσό των δεδομένων που καταγράφηκαν είναι τεράστιο και απαιτεί πολύ μεγάλο χώρο μνήμης και σύστημα, το οποίο θα πρέπει να είναι ικανό να χειρίζεται διαφορετικές μορφοποιήσεις.

2.2.5 Προστασία και διατήρηση

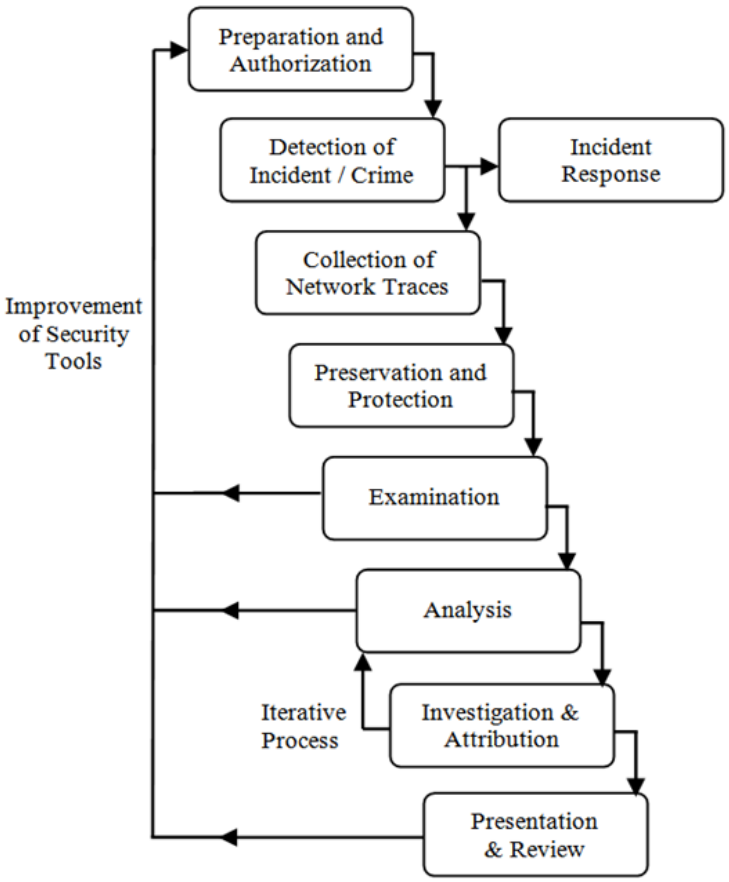
Τα αρχικά δεδομένα που αποκτήθηκαν υπό την μορφή ιχνών και αρχείων καταγραφής αποθηκεύονται σε εφεδρική συσκευή. Διατηρείται ένα αρχείο κατακερματισμού όλων των δεδομένων και προστατεύονται τα δεδομένα. Χρησιμοποιούνται πρότυπες διαδικασίες για να εξασφαλίσουν ακρίβεια και αξιοπιστία των διατηρούμενων δεδομένων. Επιβάλλεται αυστηρά η αλυσίδα φύλαξης ώστε να μην υπάρξει μη εξουσιοδοτημένη χρήση ή παραποίηση. Για την ανάλυση θα χρησιμοποιηθεί, ένα άλλο αντίγραφο των δεδομένων και τα αρχικά δεδομένα θα διατηρηθούν. Η διαδικασία αυτή πραγματοποιείται ώστε να αποδειχθεί η αυθεντικότητα των δεδομένων και να υπάρξει σύμπλευση με τις νομικές απαιτήσεις.

2.2.6 Διερεύνηση

Ενσωματώνονται τα ίχνη από διάφορους αισθητήρες ασφάλειας ώστε να διαμορφωθεί ένα μεγάλο σύνολο δεδομένων στο οποίο θα πραγματοποιηθεί η ανάλυση. Επίσης πραγματοποιείται χαρτογράφηση και διαχείριση χρόνου για την οργάνωση των δεδομένων. Αυτό πραγματοποιείται ώστε να μη χαθούν ή μπερδευτούν τα κρίσιμα δεδομένα. Τα δεδομένα αποκρύπτονται από τον επιτιθέμενο ώστε να μην ανακτηθούν. Ακόμη τα δεδομένα τα οποία συλλέγονται κατηγοριοποιούνται και χωρίζονται σε ομάδες ώστε ο όγκος των δεδομένων να αποθηκευτεί και να μειωθεί σε διαχειρίσιμες δεσμίδες δεδομένων. Με τον τρόπο αυτό είναι πιο εύκολο να αναλυθούν μεγάλες ομάδες οργανωμένων δεδομένων. Αφαιρούνται επιπλέον πληροφορίες και άσχετα δεδομένα και καθορίζονται ελάχιστα αντιπροσωπευτικά χαρακτηριστικά ώστε να γίνει ανάλυση στη μικρότερη δυνατή πληροφορία με τα περισσότερα δυνατά αποδεικτικά στοιχεία.

2.2.7 Ανάλυση

Τα αποδεικτικά στοιχεία που συλλέχθηκαν διερευνούνται μεθοδικά ώστε να εξαχθούν συγκεκριμένα υποδείγματα για το έγκλημα. Τα υποδείγματα αυτά κατηγοριοποιούνται και συσχετίζονται ώστε να εξαχθούν σημαντικές παρατηρήσεις χρησιμοποιώντας υπάρχοντα μοτίβα επιθέσεων. Χρησιμοποιούνται στοιχεία στατιστικής και εξόρυξης δεδομένων ώστε να αναζητηθούν τα δεδομένα και να αντιπαραβληθούν τα μοτίβα επίθεσης. Κάποιες από τις σημαντικές παραμέτρους σχετίζονται με την εγκαθίδρυση δικτυακής σύνδεσης, ερωτήματα DNS, κατακερματισμός πακέτων, πρωτόκολλα και αποτυπώματα λειτουργικών συστημάτων, εκτελούμενες ύποπτες διεργασίες, εγκατεστημένο λογισμικό ή rootkit. Τα μοτίβα των επιθέσεων συγχωνεύονται και η επίθεση αναδημιουργείται και επαναλαμβάνεται ώστε να κατανοηθεί η πρόθεση και η μεθοδολογία του επιτιθέμενου. Το αποτέλεσμα αυτής της φάσης είναι η επικύρωση της ύποπτης δραστηριότητας.



Εικόνα 1: Πλαίσιο για τη Δικανική Δικτύων (Pilli E., 2010)

2.2.8 Διερεύνηση και απόδοση της πηγής της επίθεσης

Η πληροφορία που αποκτήθηκε από την προηγούμενη φάση χρησιμοποιείται για να απαντήσει στα ερωτήματα της αλυσίδας φύλαξης. Αυτή η διαδικασία βοηθά στην αναζήτηση της πηγής των ιχνών, στην αναδημιουργία του σεναρίου της επίθεσης και την απόδοση της πηγής της επίθεσης. Το δυσκολότερο κομμάτι στη διερεύνηση είναι η αναγνώριση της ταυτότητας του δράστη. Δύο απλές στρατηγικές που χρησιμοποιούνται από τον εισβολέα για να αποκρύψει την ταυτότητα του είναι η παραποίηση της IP και η επίθεση σκαλοπατιών. Οι ερευνητές έχουν προτείνει πολλούς τρόπους αναζήτησης της πηγής των ιχνών για να εντοπίσουν το άτομο που ξεκίνησε την επίθεση και παραμένει ανοικτό πρόβλημα. Οι επιθέσεις σκαλοπατιών δημιουργούνται από τους επιτιθέμενους οι οποίοι χρησιμοποιούν παραβιασμένα συστήματα για να ξεκινήσουν τις επιθέσεις τους. Οι επιτιθέμενοι μπορούν να εντοπιστούν χρησιμοποιώντας προσεγγίσεις ομοιότητας και ανωμαλίας οι οποίες εφαρμόζονται σε στατιστικές πακέτων. Η προσέγγιση της διερεύνησης εξαρτάται πάντα από τον τύπο της επίθεσης.

2.2.9 Παρουσίαση και ανασκόπηση

Οι παρατηρήσεις παρουσιάζονται σε μία κατανοητή γλώσσα στις διευθύνσεις των οργανισμών και το νομικό προσωπικό, καθώς παρέχονται εξηγήσεις για τις διάφορες πρότυπες διαδικασίες που χρησιμοποιήθηκαν για να οδηγηθούν στα συμπεράσματα. Επίσης περιλαμβάνεται συστηματική τεκμηρίωση για να υπάρξει ανταπόκριση στις απαιτήσεις. Τα συμπεράσματα μπορούν επίσης να οπτικοποιηθούν ώστε να παρουσιαστούν ευκολότερα. Τα στατιστικά στοιχεία ερμηνεύονται ώστε να συνάδουν με τα συμπεράσματα. Πραγματοποιείται μία εξονυχιστική επισκόπηση του περιστατικού και προτείνονται αντίμετρα για να αποτραπούν παρόμοια περιστατικά στο μέλλον. Τα αποτελέσματα καταγράφονται για να βοηθήσουν μελλοντικές διερευνήσεις και για τη βελτίωση των προϊόντων ασφάλειας.

2.3 Σενάριο συστηματικής διερεύνησης δικτύων υπολογιστών

Στο σενάριο αυτό ένα μεγάλο υπολογιστικό σύστημα έχει παραβιαστεί, οπότε καλείται ένας εξειδικευμένος αναλυτής δικτύων ούτως ώστε να διερευνήσει την παραβίαση στο σύστημα. Ευτυχώς στην περίπτωση μας ένα σύστημα ασφαλείας δικτύου διατηρούσε όλες τις πληροφορίες των δικτυακών πακέτων τους τελευταίους έξι μήνες. Δεδομένης της μεγάλης συλλογής των δεδομένων που συλλέχθηκαν, χρειάζονται ανεπτυγμένα εργαλεία οπτικοποίησης για να εφαρμοστούν στα εκατοντάδες χιλιάδες δικτυακά συμβάντα. Αυτά τα εργαλεία σε συνδυασμό με τις πληροφορίες που συλλέχθηκαν από την διερεύνηση εκ του σύνεγγυς, χρησιμοποιούνται για την αναγνώριση των ύποπτων συνδέσεων. Μέσω της χρήσης εργαλείων οπτικοποίησης, οι ερευνητές αναγνώρισαν το εισβολέα και την παράνομη δραστηριότητα που διενεργούσε σε ένα χρονικό διάστημα έξι μηνών. Επιπρόσθετα, ανακαλύφθηκαν πρότυπα κατάχρησης του δικτύου τα οποία παρέμεναν αδιόρατα στους διαχειριστές του συστήματος, και προκλήθηκαν από άλλους εισβολείς. Η ανίχνευση τους προέκυψε μέσω ανάλυσης προτύπων. Οι επιπλέον ανωμαλίες στη χρήση του δικτύου αναγνωρίστηκαν με εξόρυξη δεδομένων και τη χρήση εργαλείων οπτικοποίησης. (Brown, 2006).

2.4. Μεθοδολογία ασφαλούς ανάκτησης και ανάλυσης διαδικτυακών δεδομένων

Στα δίκτυα όπως και στα υπολογιστικά συστήματα περιέχονται ψηφιακά αποδεικτικά στοιχεία τα οποία μπορούν να αποδείξουν την διάπραξη ενός εγκλήματος, να καθορίσουν τον τρόπο που διαπράχθηκε το έγκλημα, να παρέχουν στοιχεία στους ερευνητές, να αποκαλύψουν την σύνδεση μεταξύ του υπαιτίου και του θύματος, να διαψεύσουν ή να υποστηρίξουν τις δηλώσεις του μάρτυρα, και να ταυτοποιήσουν πιθανούς υπόπτους.

Η ανάκτηση ψηφιακών αποδεικτικών στοιχείων από την επεξεργασία σκληρών δίσκων είναι μία καλά ορισμένη διαδικασία. Ωστόσο, όταν διαχειριζόμαστε ψηφιακά αποδεικτικά στοιχεία σε ένα δίκτυο, οι ερευνητές αντιμετωπίζουν απροσδόκητες προκλήσεις. Τα δεδομένα στα δικτυωμένα συστήματα είναι δυναμικά και ευμετάβλητα, κάνοντας δύσκολη τη λήψη στιγμιότυπου στο δίκτυο για μία δεδομένη χρονική στιγμή. Σε αντίθεση με τους προσωπικούς υπολογιστές, δεν είναι εφικτό να κλείσει ένα δίκτυο διότι οι ψηφιακοί ερευνητές έχουν συνήθως την ευθύνη να εξασφαλίζουν τα αποδεικτικά στοιχεία χωρίς να αποδιοργανώσουν τις επιχειρηματικές δραστηριότητες που

βασίζονται στο δίκτυο. Εξάλλου, το κλείσιμο του δικτύου θα οδηγήσει στην καταστροφή των περισσότερων ψηφιακών αποδεικτικών στοιχείων που περιέχονται σε αυτό. Επίσης λόγω της ποικιλομορφίας των τεχνολογιών δικτύωσης αλλά και των υποσυστημάτων του δικτύου, συχνά κρίνεται απαραίτητο να εφαρμόσουμε τις καλύτερες τεχνικές συλλογής αποδεικτικών στοιχείων σε ασυνήθιστο περιεχόμενο.

Επιπρόσθετα, αντίθετα από τα εγκλήματα στο φυσικό περιβάλλον, τα ψηφιακά εγκλήματα μπορούν να πραγματοποιηθούν σε διαφορετικά σημεία ενός δικτύου σε οποιαδήποτε χρονική στιγμή. Η κατανομή της εγκληματικής δραστηριότητας και τα συσχετισμένα με αυτή αποδεικτικά στοιχεία κάνουν δύσκολη την απομόνωση ενός εγκλήματος. Βέβαια την ίδια στιγμή, δεδομένου ότι τα αποδεικτικά στοιχεία είναι διεσπαρμένα σε πολλούς υπολογιστές, οι ψηφιακοί ερευνητές μπορούν να έχουν πλεονέκτημα κατά την διερεύνηση. Αυτή η κατανομή των πληροφοριών είναι που κάνει δύσκολη την καταστροφή των ψηφιακών αποδεικτικών στοιχείων. Εάν καταστραφούν τα ψηφιακά αποδεικτικά στοιχεία σε ένα υπολογιστικό σύστημα, συχνά μπορεί να βρεθεί ένα αντίγραφο τους σε διάφορους υπολογιστές στο δίκτυο. Αυτό το γεγονός το παρατηρούμε στις επιχειρήσεις, όπου διατηρούν τακτικά εφεδρικά αντίγραφα ασφάλειας των δεδομένων τους και σε ορισμένες περιπτώσεις αποθηκεύουν ένα δεύτερο εφεδρικό αντίγραφο σε διαφορετική τοποθεσία για επαυξημένη προστασία.

Η αναζήτηση για πηγές ψηφιακών αποδεικτικών στοιχείων στα δίκτυα απαιτεί την διεύρυνση του πεδίου αναζήτησης και συχνά οδηγούμαστε σε τύπους δεδομένων οι οποίοι απαιτούν εξειδικευμένους εμπειρογνώμονες για να συλλεχθούν. Η συστηματική διερεύνηση δικτύων απαιτεί προσαρμογή στις διαφορετικές τεχνολογίες και ιδιότητες των δικτύων. Επιπλέον η ανάλυση των ψηφιακών αποδεικτικών στοιχείων στα δίκτυα απαιτεί συνήθως εξειδικευμένη γνώση των εργαλείων και της υποκείμενης τεχνολογίας δικτύου. Η παρουσίαση των αποτελεσμάτων της έρευνας σε μη εξειδικευμένο κοινό αποτελεί πρόκληση αλλά παραμένει ένα από τα πλέον σημαντικά στάδια της συστηματικής διερεύνησης καθώς τα αποτελέσματα του ερευνητή μπορεί να παραμείνουν αχρησιμοποίητα αν δε γίνουν κατανοητά. Στη συνέχεια θα παρουσιαστούν το καθένα από τα στάδια της συστηματικής διερεύνησης δικτύων, εξετάζοντας την εφαρμογή των ψηφιακών αποδεικτικών στοιχείων στα δίκτυα υπολογιστών.

2.4.1 Προετοιμασία και Εξουσιοδότηση

Σε κάποιες περιπτώσεις τα ψηφιακά αποδεικτικά στοιχεία παραμένουν σε δίκτυα που δεν έχουν απευθείας ανάμειξη σε ένα έγκλημα όποτε οι διαχειριστές αυτών των δικτύων είναι συνεργάσιμοι και συχνά βοηθούν τους ψηφιακούς ερευνητές στη συλλογή αποδεικτικών στοιχείων. Επίσης ορισμένοι διαχειριστές συστημάτων καταγράφουν τακτικά χρήσιμα δεδομένα ώστε να ανακαλύψουν και να επιλύσουν προβλήματα απόδοσης και ασφάλειας, συλλέγοντας προληπτικά αποδεικτικά στοιχεία. Επιπλέον, σε ένα δίκτυο υπάρχουν περισσότερες πηγές ψηφιακών αποδεικτικών στοιχείων γεγονός το οποίο δεν αντιλαμβάνονται οι διαχειριστές συστημάτων. Επομένως για να εξασφαλιστεί ότι όλα τα σχετιζόμενα δεδομένα έχουν εντοπιστεί, οι ψηφιακοί ερευνητές πρέπει να χρησιμοποιήσουν εκτενώς τις γνώσεις τους για τα δίκτυα ώστε μετά από συνεργασία με τους διαχειριστές συστημάτων να έχουν καθαρή εικόνα των ψηφιακών αποδεικτικών στοιχείων που θα χρειαστούν.

Στην περίπτωση που δεν αναμένεται συνεργασία από τον διαχειριστή συστήματος, οι ψηφιακοί ερευνητές θα πρέπει να αποκτήσουν από μόνοι τους πληροφορίες για τα συστήματα, πριν ακόμη λάβουν εξουσιοδότηση για τη συλλογή ψηφιακών αποδεικτικών στοιχείων. Επιπλέον είναι χρήσιμο για τους ερευνητές να μάθουν τους τύπους των υπολογιστικών συστημάτων που χρησιμοποιούνται ώστε να γνωρίζουν εκ των προτέρων τα εργαλεία που θα τους χρειαστούν. Η συλλογή ψηφιακών αποδεικτικών στοιχείων από ένα μεγάλο δίκτυο απαιτεί σημαντικό προγραμματισμό, ειδικότερα εάν οι διαχειριστές των συστημάτων δεν είναι συνεργάσιμοι. Η απόκτηση πληροφορίας από τα συστήματα προς διερεύνηση, πριν από την πραγματική διερεύνηση μπορεί να εξελιχθεί σε χρονοβόρα διαδικασία. Η διαδικασία συλλογής πληροφοριών από ένα δίκτυο μπορεί να περιλαμβάνει επισκόπηση των παραγγελιών, μελέτη των αναφορών ελέγχου ασφάλειας, εξ αποστάσεως διερεύνηση του συστήματος, εξέταση των κεφαλίδων των μηνυμάτων ηλεκτρονικού ταχυδρομείου, αναζήτηση στο διαδίκτυο, στο Usenet, στο DNS και σε άλλες πηγές διαδικτύου που θα αποκαλύψουν λεπτομέρειες στο δίκτυο.

Τα εργαλεία συλλογής πληροφοριών, που χρησιμοποιούνται για την εξ αποστάσεως διερεύνηση των υπολογιστικών συστημάτων, μπορεί να ενεργοποιήσουν ένα μηχανισμό ειδοποίησης εάν το σύστημα χρησιμοποιεί τείχος προστασίας ή σύστημα ανίχνευσης παρείσφρησης. Επιπλέον κάποια εργαλεία θα διαταράξουν τα συστήματα και θα πρέπει να χρησιμοποιηθούν μόνο από εκπαιδευμένο

προσωπικό με επαρκή αρμοδιότητα. Επομένως, πριν γίνει απευθείας σύνδεση με το σύστημα του υπόπτου, οι ψηφιακοί ερευνητές θα πρέπει να ισοσταθμίσουν τη σημαντικότητά της πληροφορίας με το ρίσκο να εγείρουν ανησυχία στον ύποπτο.

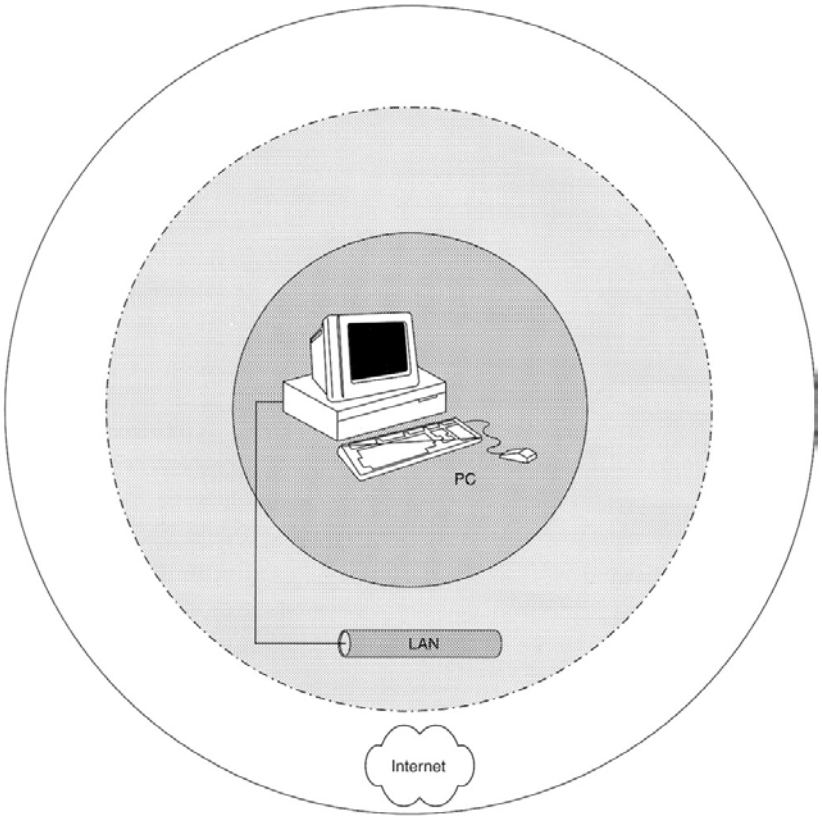
IP ADDRESS	HOSTNAME	FUNCTION	DIGITAL EVIDENCE	TYPE/VERSION	PRIORITY	NOTES
192.168.1.32	mail.corpX.com	SMTP/POP/IMAP	Suspect's e-mail content, logs, backup tapes, syslogs	Solaris 8	3	Too large to copy entire disk. Just copy e-mail logs
192.168.1.33	dc1.corpX.com	Domain controller	NT Event, IAS, and IIS logs	Windows 2000	3	
192.168.1.34	www.corpX.com	WWW, shell	Web and shell access logs, syslogs, config files	Redhat Linux 8	3	Web access logs in /data /logs
192.168.1.42	ids.corpX.com	Snort IDS	Snort logs and configuration files, syslogs and system config files/details	FreeBSD 5	2	Logs backed up daily to compact disk
192.168.1.45	flow.corpX.com	NetFlow Collectoror	NetFlow logs in raw and text format	Solaris 8	2	Also stored in Oracle database to facilitate searching
192.168.52.23	srv1.corpX.com	File server	Bitstream copy of disk	Windows NT 4	1	
192.168.98.34	wks34.corpX.com	Suspect's Workstation	Bitstream copy of disk	Windows NT 4	1	

Πίνακας 1: Υπόδειγμα που δημιουργήθηκε για την προετοιμασία συλλογής ψηφιακών αποδεικτικών στοιχείων από ένα μικρό εταιρικό δίκτυο (Casey, 2004).

2.4.2 Αναγνώριση

Κατά την ενασχόληση μας με τους υπολογιστές σαν πηγές αποδεικτικών στοιχείων, η διερεύνηση στον τόπο του εγκλήματος συχνά οδηγεί σε διασυνδεδεμένα δίκτυα και τελικά στο διαδίκτυο. Αντιστρόφως όταν οι ψηφιακοί ερευνητές αναζητούν αποδεικτικά στοιχεία στο διαδίκτυο, η

αναζήτηση τους οδηγεί σε μικρότερα ιδιωτικά δίκτυα μέχρι και σε μεμονωμένους υπολογιστές. Αυτοί οι τομείς διερεύνησης απεικονίζονται στο παρακάτω σχήμα με διακεκομμένες γραμμές ανάμεσα στο διαδίκτυο και στο μικρότερο ιδιωτικό δίκτυο γιατί δεν υπάρχει σαφής διαχωρισμός ανάμεσα σε αυτά τα δύο. Για παράδειγμα, τα εταιρικά δίκτυα έχουν συνήθως διακομιστές που χρησιμοποιούνται για τον διαμοιρασμό πληροφοριών μέσα στον οργανισμό και αυτοί οι διακομιστές είναι συχνά προσβάσιμοι στους εργαζόμενους μέσω του διαδικτύου.



Εικόνα 2: Τομείς διερεύνησης που μπορεί να περιέχουν ψηφιακά αποδεικτικά στοιχεία (Casey, 2004).

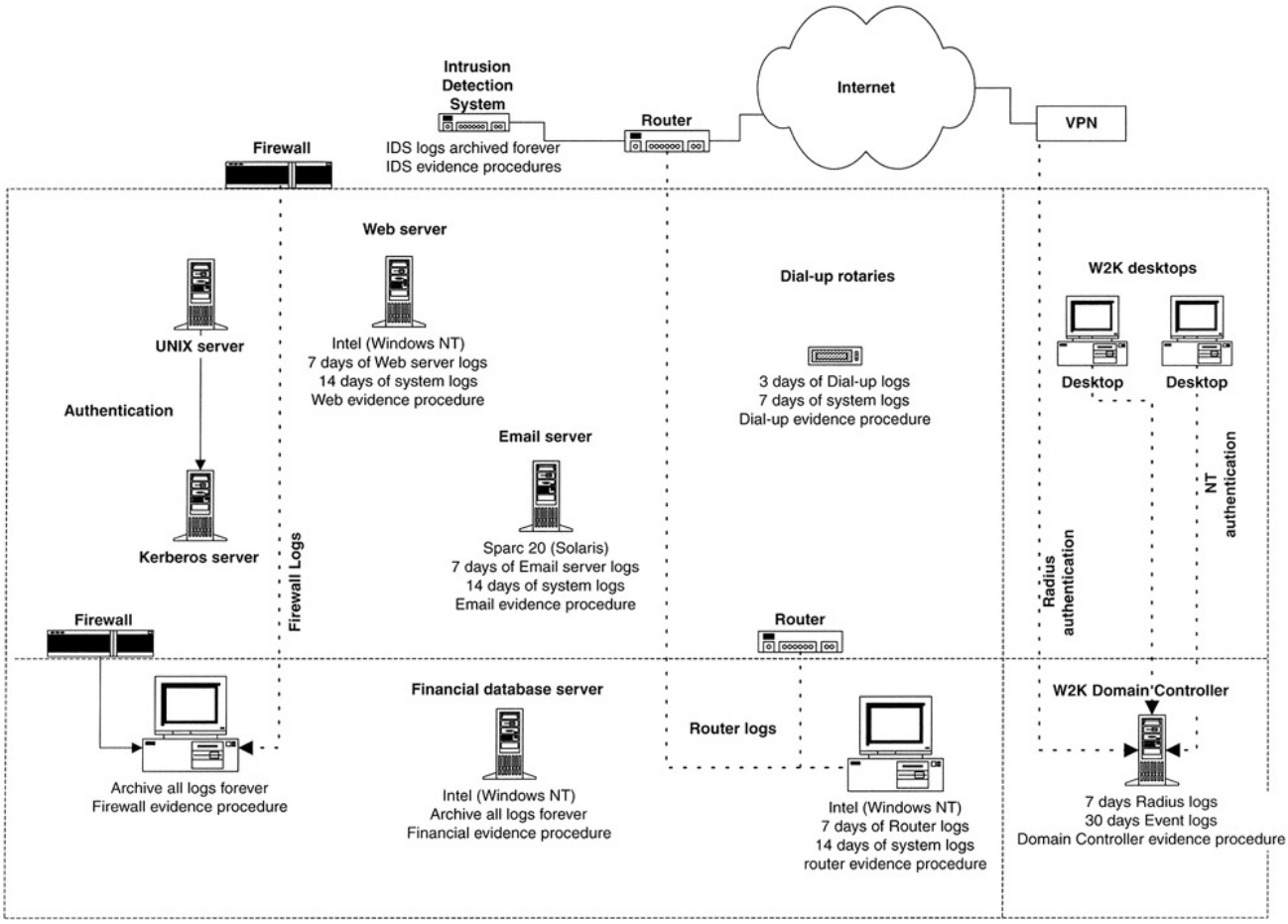
Δεδομένου του μεγάλου πλήθους πληροφοριών που ενυπάρχουν σε αυτές τις περιοχές, κρίνεται απαραίτητη η χρήση μίας μεθόδου γρήγορου εντοπισμού συστημάτων που περιέχουν τα πιο χρήσιμα ψηφιακά αποδεικτικά στοιχεία. Η πρώτη φάση είναι η διερεύνηση των τερματικών κόμβων και των ενδιάμεσων συστημάτων όπως μεταγωγείς, δρομολογητές και proxy. Αυτά τα συστήματα μπορεί να περιέχουν ψηφιακά αποδεικτικά στοιχεία που βοηθούν να καθορίσουμε τη συνέχεια του αδικήματος και να αποκτήσουμε μία καλύτερη κατανόηση του εγκλήματος. Για παράδειγμα κατά την αποστολή μηνυμάτων παρενόχλησης μέσω ηλεκτρονικού ταχυδρομείου, τα αρχεία καταγραφής στον διακομιστή ηλεκτρονικού ταχυδρομείου που χρησιμοποιήθηκε για την αποστολή τους, μπορεί να

μας δώσει πλήρη γνώση των ενεργειών του υπόπτου από ένα και μόνο μήνυμα. Επιπλέον τα ενδιάμεσα συστήματα όπως οι δρομολογητές και οι μεταγωγείς μπορούν να δημιουργήσουν λεπτομερή αρχεία καταγραφής της δικτυακής κίνησης, που μας οδηγεί στην δεύτερη φάση. Οι διεργασίες που εκτελούνται στην δεύτερη φάση είναι η αναζήτηση των αρχείων καταγραφής που παρέχουν πλήρη εικόνα των ενεργειών στο δίκτυο, όπως αρχεία καταγραφής πακέτων που παρέχονται από τα συστήματα παρακολούθησης κίνησης δικτύου, αρχεία καταγραφής κίνησης δικτύου που παρέχονται από τη διερεύνηση μέσω του Argus, αρχεία καταγραφής των δρομολογητών και αρχεία καταγραφής προειδοποιήσεων που παρέχονται από τα συστήματα ανίχνευσης παρείσφρησης. Τα αρχεία καταγραφής επιπέδου δικτύου είναι πολύ χρήσιμα για τον καθορισμό των συμβάντων καθώς και των άλλων εμπλεκόμενων συστημάτων. Για παράδειγμα, κατά τη διερεύνηση μιας εισβολής σε ένα υπολογιστικό σύστημα, τα αρχεία καταγραφής επιπέδου δικτύου μπορούν να αποκαλύψουν ότι ο ίδιος ο εισβολέας είχε ως στόχο και μερικά άλλα συστήματα του δικτύου. Κατά την τρίτη φάση αναζητούμε συστήματα υποστήριξης, όπως διακομιστές αυθεντικοποίησης και συστήματα αναγνώρισης κληθέντος, τα οποία μπορούν να αντιστοιχίσουν τις διαδικτυακές δραστηριότητες με ένα άτομο. Στην πράξη αυτές οι τρεις φάσεις διεξάγονται ταυτόχρονα δεδομένου ότι σε κάποιες περιπτώσεις η δεύτερη και τρίτη φάση μπορεί να μας οδηγήσουν σε άλλα ενδιάμεσα ή τερματικά συστήματα. Η προσέγγιση των τριών φάσεων είναι χρήσιμη όταν εστιάζουμε στην αναζήτηση ψηφιακών αποδεικτικών στοιχείων σε ένα δίκτυο ώστε να ανακατασκευάσουμε την εγκληματική δραστηριότητα.

Είναι συχνά απαραίτητο να αναλυθούν άμεσα τα αποδεικτικά στοιχεία ώστε να εντοπιστούν άλλες πηγές αποδεικτικών στοιχείων και να συλληφθεί ο υπαίτιος. Κατά την διερεύνηση είναι περισσότερο αποτελεσματικό να συλλέγονται τα αποδεικτικά στοιχεία από μία ομάδα και στην συνέχεια να αναλύονται άμεσα από μία δεύτερη ομάδα, παρά να ανατίθεται όλο το έργο της συλλογής και ανάλυσης στοιχείων σε ένα μόνο άτομο. Αυτό το ζήτημα περιπλέκεται όταν ασχολούμαστε με συσκευές όπως δρομολογητές διότι το αποτελέσματα μίας εντολής συχνά βοηθά τους ψηφιακούς ερευνητές να καθορίσουν ποια άλλη πληροφορία πρέπει να συλλέξουν από τη μνήμη και ποια εντολή να εκτελέσουν στη συνέχεια, γεγονότα που απαιτούν ταυτόχρονη συλλογή και ανάλυση. Σε αυτές τις περιπτώσεις υπάρχει ανάγκη πρότυπων διαδικασιών για τη συλλογή αποδεικτικών στοιχείων. Βέβαια η ανάπτυξη πρότυπων διαδικασιών μπορεί να μην είναι εφικτή για όλες τις διαδικτυακές συσκευές που μπορεί να συναντήσουμε, αλλά για τις περισσότερο συνηθισμένες όπως για δρομολογητές Cisco και τείχη προστασίας.

Δεδομένης της εκτεταμένης περιοχής έρευνας, το ενδεχόμενο λαθών, αλλά και τη μεγάλη ποικιλία των ψηφιακών αποδεικτικών στοιχείων στα δίκτυα κρίνεται απαραίτητη η χρήση μιας μεθοδικής προσέγγισης κατά την αναζήτηση αποδεικτικών στοιχείων στα δίκτυα. Αν και είναι απαραίτητο να ακολουθούμε τα διαδικτυακά ίχνη, δεν κρίνεται επαρκές για τον εντοπισμό πηγών των ψηφιακών αποδεικτικών στοιχείων τα οποία δεν σχετίζονται άμεσα με την διάπραξη ενός εγκλήματος, αλλά περιέχουν δεδομένα σχετικά με το έγκλημα. Για παράδειγμα πολλοί δρομολογητές είναι ρυθμισμένοι να στέλνουν τα αρχεία καταγραφής σε απομακρυσμένους διακομιστές σε μόνιμο αποθηκευτικό χώρο, γεγονός που είναι χρήσιμο για τους ψηφιακούς ερευνητές ώστε να συλλέξουν χρήσιμα ψηφιακά δεδομένα, παραμερίζοντας προς στιγμή τα διαδικτυακά ίχνη.

Η μεθοδική διερεύνηση μπορεί να διευκολυνθεί με μία γραφική αποτύπωση του δικτύου όπου είναι αποθηκευμένες ενδεχόμενες πηγές αποδεικτικών στοιχείων. Ένα απλοϊκό υπόδειγμα φαίνεται παρακάτω.



Εικόνα 3: Υπόδειγμα χάρτη ψηφιακών αποδεικτικών στοιχείων (Casey, 2004).

Πολλοί οργανισμοί έχουν διαγράμματα τοπολογίας δικτύου τα υποδεικνύουν τον τρόπο διασύνδεσης των σημαντικότερων υποσυστημάτων του δικτύου. Αυτά τα διαγράμματα δικτύου μπορούν να χρησιμοποιηθούν ως σημείο εκκίνησης κατά την ανάπτυξη ενός χάρτη ψηφιακών αποδεικτικών στοιχείων, χωρίς να παραγνωρίζεται το γεγονός ότι συχνά αυτά τα διαγράμματα δεν είναι ενημερωμένα και σπάνια είναι αρκετά λεπτομερή για να καλύψουν τις ανάγκες των ψηφιακών ερευνητών.

Επομένως, αντλώντας πληροφορίες από ανθρώπους που είναι εξοικειωμένοι με το υπάρχων δίκτυο αλλά και από πληροφορίες που συλλέχθηκαν κατά το προπαρασκευαστικό στάδιο της διερεύνησης μπορεί να αναπτυχθεί μία ακριβής αποτύπωση του δικτύου και των υποσυστημάτων του.

Ο εντοπισμός των σημείων εισόδου σε ένα δίκτυο καθώς και οι διακομιστές κλειδιά συχνά οδηγούν στις πλουσιότερες πηγές ψηφιακών αποδεικτικών στοιχείων. Όταν αναγνωριστούν οι σημαντικότεροι διακομιστές και διαδικτυακές συσκευές, οι ψηφιακοί ερευνητές μπορούν να καθορίσουν ποια δεδομένα θα διατηρήσουν στο δίσκο και στη μνήμη, στα σημεία όπου είναι αποθηκευμένα τα αρχεία καταγραφής, τα αρχεία ρυθμίσεων και τα εφεδρικά αντίγραφα. Πριν εξάγουμε από τη διερεύνηση ένα σύστημα ως ενδεχόμενη πηγή αποδεικτικών στοιχείων, θα πρέπει να σιγουρευτούμε ότι εξετάσαμε τη διαδικτυακή συσκευή εκτενώς μιας και τα αποδεικτικά στοιχεία μπορεί να βρεθούν σε απροσδόκητα σημεία. Για παράδειγμα, εάν οι δρομολογητές σε ένα δεδομένο δίκτυο διατηρούν μόνο αρχεία καταγραφής δυσλειτουργιών, πρέπει να ελέγξουμε εάν οι δυσλειτουργίες προσφέρουν κάποια σημαντική πληροφορία. Ο χάρτης ψηφιακών αποδεικτικών στοιχείων θα πρέπει να συνοψίζει ποιες πληροφορίες μπορούν να βρεθούν σε κάθε κόμβο του δικτύου για πόσο καιρό διατηρούνται τα αποδεικτικά στοιχεία και πως μπορούν να ανακτηθούν. Αυτές οι πληροφορίες ενεργοποιούν τους ερευνητές ώστε να δώσουν προτεραιότητα στα περισσότερο ευπαθή αποδεικτικά στοιχεία.

2.4.3 Τεκμηρίωση, Συλλογή, και Διατήρηση

Σε κάποιες περιπτώσεις είναι επιθυμητή η διατήρηση των ψηφιακών αποδεικτικών στοιχείων από ένα δίκτυο, αποκτώντας φυσική πρόσβαση στο ζητούμενο υπολογιστικό σύστημα και αντιγράφοντας τα δεδομένα σε δέσμες bit. Επίσης ακολουθείται η ίδια διαδικασία σε περιπτώσεις όπου

διατηρούνται δεδομένα σε αποθηκευτικά μέσα και για την ανάγνωση τους χρειάζεται εξειδικευμένο υλικό και λογισμικό.

Η αντιγραφή δεσμίδων bit μπορεί να μην είναι εφικτή σε κάποιες περιπτώσεις όπου το σύστημα δεν μπορεί να τερματιστεί, ή ο σκληρός δίσκος είναι πολύ μεγάλος για να αντιγραφεί, ή ο ψηφιακός ερευνητής δεν έχει την απαραίτητη εξουσιοδότηση για να αντιγράψει ολόκληρο το δίσκο. Επίσης, οι ψηφιακοί ερευνητές είναι συχνά εξαρτημένοι από μεγάλους παρόχους διαδικτύου, περιμένοντας να τους παρέχουν αποδεικτικά στοιχεία όπως πληροφορίες για τους συνδρομητές τους. Ακόμη οι ψηφιακοί ερευνητές μπορεί να μην έχουν φυσική πρόσβαση στο σύστημα που περιέχει τα αποδεικτικά στοιχεία, αναγκάζοντάς τους να συλλέξουν τα αποδεικτικά στοιχεία εξ αποστάσεως. Επίσης στην περίπτωση όπου υπάρχει μεγάλη πιθανότητα να καταστραφούν τα δεδομένα προτού φθάσουν στο σύστημα, τότε οι ψηφιακοί ερευνητές θα συλλέξουν τα ψηφιακά αποδεικτικά στοιχεία εξ αποστάσεως. Για παράδειγμα, δεδομένα όπως ιστοσελίδες και μηνύματα Usenet μπορεί να μεταβληθούν ή να καταστραφούν σε οποιαδήποτε χρονική στιγμή. Να σημειώσουμε επίσης ότι οι εισβολείς υπολογιστικών συστημάτων συνήθως διαγράφουν τα αρχεία καταγραφής.

Επίσης, όταν οι ψηφιακοί ερευνητές εκτελούν συγκεκριμένες ενέργειες, τα δεδομένα παρουσιάζονται στην οθόνη μόνο για μια στιγμή, κάνοντας με τον τρόπο αυτό απαραίτητη την καταγραφή των δυναμικών αποδεικτικών στοιχείων. Για παράδειγμα προγράμματα σε UNIX αλλά και το HyperTerminal για συστήματα Microsoft Windows μπορούν να χρησιμοποιηθούν για να καταγράψουν τα αποτελέσματα της ανάλυσης των δρομολογητών, των τειχών προστασίας, και άλλων δικτυακών συσκευών με τη χρήση σειριακού καλωδίου. Επίσης, ένας δεύτερος ερευνητής μπορεί να παρακολουθεί τη διαδικασία της συλλογής και να καταγράφει την κάθε ενέργεια και το αποτέλεσμά της καθώς συλλέγονται τα αποδεικτικά στοιχεία. Αυτή η προσέγγιση μπορεί να βοηθήσει ώστε να αναγνωριστούν άμεσα τα λάθη και να γίνουν αντιπροτάσεις.

Ένα άλλο παράδειγμα συλλογής αποδεικτικών στοιχείων σε πραγματικό χρόνο είναι μία σύνοδος IRC κατά την οποία οι ψηφιακοί ερευνητές διατηρούν ένα ενεργό αρχείο καταγραφής της συζήτησης με τον ύποπτο. Ωστόσο, εάν ένα αξιοσημείωτο ποσό πληροφορίας παρουσιάζεται στην οθόνη, μπορεί να είναι επιθυμητή η οπτική αναπαράσταση των γεγονότων. Μια οπτική καταγραφή μπορεί να γίνει χρησιμοποιώντας κάμερα ή ένα πρόγραμμα που μπορεί να καταγράψει δυναμικά μεταβαλλόμενα αποδεικτικά στοιχεία, σαν μία σειρά γεγονότων στην οθόνη, και μπορούν να

αναπαραχθούν σε ένα μεταγενέστερο χρονικό σημείο. Να σημειώσουμε ότι αυτά και άλλα προγράμματα που είναι χρήσιμα για τη συλλογή ψηφιακών αποδεικτικών στοιχείων δεν εκτελούν έλεγχο ακεραιότητας ή κάποια άλλη τεκμηρίωση ούτως ώστε να αυθεντικοποιηθούν τα δεδομένα.

Μία λεπτομερής καταγραφή της συνολικής διαδικασίας συλλογής θα πρέπει να διατηρηθεί σε ψηφιακή και γραπτή μορφή ώστε να βοηθήσει στην αυθεντικοποίηση των αντιγράφων σε μεταγενέστερο χρόνο. Η καταγραφή αυτή θα πρέπει να τεκμηριώνει ποιος συνέλεξε τα αποδεικτικά στοιχεία, πως, πότε και γιατί. Με δεδομένη την κατανεμημένη φύση του διαδικτύου και τις πολλές ενδεχόμενες πηγές ψηφιακών αποδεικτικών στοιχείων, αποτελεί μεγάλη πρόκληση ακόμα και η συλλογή των σχετικά στατικών αποδεικτικών στοιχείων όπως για παράδειγμα οι ιστοσελίδες και τα μηνύματα Usenet. Σε αυτές τις απλές περιπτώσεις, μπορεί να μην είναι δυνατή η απόκτηση των ιδιοτήτων του χρόνου και ημερομηνίας των συσχετιζόμενων αρχείων στο απομακρυσμένο σύστημα. Επομένως, είναι επιτακτικό να κάνουμε κάθε δυνατή προσπάθεια ώστε να τεκμηριωθεί το γεγονός ότι τα αποδεικτικά στοιχεία αποθηκεύθηκαν στο απομακρυσμένο σύστημα, περιγράφοντας λεπτομερώς την τοποθεσία των αρχικών αποδεικτικών στοιχείων, πότε, πως και από ποιόν συλλέχθηκαν. Στις περισσότερο περίπλοκες καταστάσεις, γίνεται ολοένα και αυξανόμενη η πρόκληση της καταγραφής των αποδεικτικών στοιχείων, όπως αυτά συλλέχθηκαν από το απομακρυσμένο σύστημα.

Ανάλυση περίπτωσης:

Ένας εισβολέας έχει ανιχνευθεί ότι έχει παραβιάσει ένα υπολογιστικό σύστημα ενός οργανισμού μέσω διαδικτύου. Πριν αποσυνδεθεί από το σύστημα, οι ψηφιακοί ερευνητές συνέλεξαν αποδεικτικά στοιχεία που αποδείκνυαν ότι ο εισβολέας διέπραξε το έγκλημα. Για να εξασφαλίσουν στοιχεία ισοδύναμα με την βιντεοσκόπηση του υπόπτου να διαπράττει το έγκλημα, οι ψηφιακοί ερευνητές χρησιμοποίησαν ένα sniffer ώστε να παρακολουθήσουν την κίνηση δικτύου καταγράφοντας όλα τα πακέτα IP κατά τη σύνδεση του εισβολέα. Επιπλέον, συνδέθηκαν με το εκτεθειμένο σύστημα χρησιμοποιώντας ένα πρόγραμμα το οποίο διατηρούσε αρχείο καταγραφής κατά την σύνοδο και συνέλεξε αποδεικτικά στοιχεία από τις ενέργειες του εισβολέα στο σύστημα αλλά και τα προγράμματα που εκτέλεσε. Σε μία προσπάθεια αναζήτησης σχετικών αποδεικτικών στοιχείων, οι ψηφιακοί ερευνητές αναζήτησαν στα γειτονικά συστήματα πληροφορίες σχετιζόμενες με τον εισβολέα. Ανακάλυψαν ότι και τα υπόλοιπα είχαν παραβιαστεί από τον ίδιο εισβολέα και συνδέθηκε

σε αυτά μέσω ενός κενού ασφαλείας το οποίο εκμεταλλεύθηκε ο εισβολέας. Λόγω του γεγονότος ότι δεν ήταν δυνατή η πρόσβαση των ερευνητών σε όλα τα εκτεθειμένα συστήματα με φυσικό τρόπο και επίσης υπήρχε το ρίσκο ότι ο εισβολέας μπορεί να κατέστρεφε τα αποδεικτικά στοιχεία στα συστήματα σε οποιοδήποτε χρονική στιγμή, οι ψηφιακοί ερευνητές συνέλεξαν τα αποδεικτικά στοιχεία εξ αποστάσεως. Καθώς εκτελούσαν την εξ αποστάσεως συλλογή, χρησιμοποίησαν και πάλι λογισμικό που κατέγραφε τις πληκτρολογήσεις, με αποτέλεσμα την τεκμηρίωση της διαδικασίας συλλογής.

Όταν είναι απαραίτητη η σύνδεση μέσω δικτύου σε ένα υπολογιστικό σύστημα, αλλά και η συλλογή αποδεικτικών στοιχείων από το σύστημα, θα πρέπει να έχουμε επίγνωση για κάποια ζητήματα, και μερικούς τρόπους οι οποίοι βοηθούν στην τεκμηρίωση της διαδικασίας και επιδεικνύουν ακεραιότητα και αυθεντικοποίηση:

1. Χρησιμοποίηση μίας πρότυπης διαδικασίας λειτουργίας. Με τον τρόπο αυτό μειώνονται τα σφάλματα και αυξάνεται η συνέπεια της διερεύνησης.

2. Είναι απαραίτητη η διατήρηση ενός αρχείου καταγραφής των ενεργειών που ακολουθήθηκαν κατά τη διαδικασία συλλογής και η αποθήκευση στιγμιότυπων οθόνης για τα πιο σημαντικά στοιχεία.

3. Θα πρέπει να τεκμηριωθεί ποιος διακομιστής περιείχε τα δεδομένα τα οποία συλλέχθηκαν, διότι ο ερευνητής μπορεί να προωθηθεί από ένα διακομιστή σε έναν άλλον σε διαφορετική χώρα.

4. Υπολογισμός των τιμών σύνοψης MD5 ή SHA1 όλων των αποδεικτικών στοιχείων πριν τη μεταφορά τους, καθώς και μετά τη μεταφορά τους από το απομακρυσμένο σύστημα.

5. Όσον αφορά τα αρχεία που συλλέχθηκαν θα πρέπει να υπογραφούν ψηφιακά, να κρυπτογραφηθούν και να αποθηκευθούν ως αρχεία μόνο για ανάγνωση.

Τα περισσότερα εργαλεία ανάλυσης μπορούν να μετατρέψουν τα αρχεία σε μορφή tcpdump. Η συλλογή της κίνησης δικτύου χρήζει επίσης ειδικής μεταχείρισης. Εάν η διεύθυνση IP για την οποία

ενδιαφερόμαστε είναι ήδη γνωστή, τότε η καταγραφή της διαδικτυακής κίνησης που αφορά μόνο αυτόν τον υπολογιστή είναι απλό ζήτημα. Ωστόσο εάν η IP ανατίθεται δυναμικά σε ένα δίκτυο, μπορεί να είναι απαραίτητη η παρακολούθηση της κίνησης από μία συγκεκριμένη διεύθυνση MAC. Σε άλλες περιπτώσεις μπορεί να είναι απαραίτητη η παρακολούθηση της κίνησης σε όλο το δίκτυο.

Κατά την καταγραφή της δικτυακής κίνησης, μπορεί να είναι επιθυμητό να περιοριστεί το ποσό και ο τύπος της πληροφορίας που συλλέγεται. Για παράδειγμα, οι ψηφιακοί ερευνητές μπορεί να έχουν εξουσιοδότηση για να παρακολουθήσουν μόνο την κίνηση μέσω του ιστού. Παρόλο που κάποια εργαλεία καταγραφής δικτυακής κίνησης μπορούν να ρυθμιστούν ούτως ώστε να συλλέγουν μόνο την κίνηση μέσω ιστού, μερικά από αυτά υποθέτουν ότι εμπλέκονται μόνο συγκεκριμένες θύρες, ενώ άλλα εργαλεία αναγνωρίζουν με επιτυχία τα πρωτόκολλα που χρησιμοποιούνται. Αυτό το φιλτράρισμα αποδεικνύεται δύσκολο όταν τα πρωτόκολλα μοιάζουν μεταξύ τους. Για παράδειγμα ορισμένα πρωτόκολλα P2P είναι βασισμένα στο HTTP, και κάποια προγράμματα άμεσων μηνυμάτων προσπαθούν να προσομοιάσουν την κίνηση μέσω ιστού για να παρακάμψουν τα τείχη προστασίας. Επομένως θα πρέπει πρώτα να γίνεται η συλλογή και στη συνέχεια το φιλτράρισμα και η ανάλυση, όποτε αυτό είναι δυνατό.

2.4.4 Φιλτράρισμα και αφαίρεση δεδομένων

Οι διερευνήσεις οι οποίες περιλαμβάνουν υπολογιστικά συστήματα συχνά οδηγούν σε μεγάλο όγκο δεδομένων, τα περισσότερα από τα οποία δεν έχουν σχέση με την διερεύνηση που διεξάγεται. Επίσης όταν ασχολούμαστε με αρχεία που συλλέχθηκαν μέσω κίνησης δικτύου, οι ψηφιακοί ερευνητές θα πρέπει να αγνοήσουν ή να διαγράψουν τα αρχεία για τα οποία δεν έχουν προνόμια χρήσης ή είναι απόρρητα. Επομένως το φιλτράρισμα των δεδομένων και η αφαίρεση δεδομένων είναι απαραίτητες διαδικασίες κατά τη διερεύνηση δικτύων ώστε να επιτύχουμε αποδοτική και εκτενή ανάλυση των αποδεικτικών στοιχείων.

Το φιλτράρισμα των δεδομένων από τα αρχεία καταγραφής μπορεί να είναι τόσο απλό όσο η εξαγωγή καταχωρήσεων που ταιριάζουν με συγκεκριμένα κριτήρια όπως ένα συγκεκριμένο χρονικό διάστημα, μία διεύθυνση IP, ή αποτυχημένα γεγονότα σύνδεσης στο σύστημα. Για παράδειγμα στο παρακάτω αρχείο εξόδου εμφανίζονται μόνο αποτυχημένα γεγονότα σύνδεσης που σχετίζονται με

τον χρήστη "eco", όπως έγινε η εξαγωγή τους από το Windows NT Event Log χρησιμοποιώντας το εργαλείο ntlast.

C:\>ntlast -f -u eco -file e:\case1\dc2\sec.evt

eco	*WORKSTN13*	*MY-DOMAIN*	*Sun Jan 19 11:00:11 am 2003*
eco	*WORKSTN10*	*MY-DOMAIN*	*Wed Jan 15 05:39:39 pm 2003*

Όταν εξετάζονται οι συνδέσεις που εγκαθιδρύθηκαν, μέσω ενός τείχους προστασίας Cisco PIX, είναι επιθυμητό να επικεντρωθούμε σε ένα υπολογιστή παρά σε κάθε σύνδεση χωριστά. Παρακάτω βλέπουμε ένα παράδειγμα.

pix01# show conn foreign 192.168.0.232 255.255.255.255
7354 in use, 24529 most used
TCP out 192.168.0.232:3129 in 172.16.1.23:80 idle 0:12:04 Bytes 45235 flags UIO
TCP out 192.168.0.232:3130 in 172.16.1.23:22 idle 0:00:01 Bytes 4395 flags UIO
TCP out 192.168.0.232:3131 in 172.16.1.23:443 idle 0:00:54 Bytes 9935 flags UIO

Ωστόσο αυτή η προσέγγιση της συλλογής αποδεικτικών στοιχείων από ένα τείχος προστασίας, παραβιάζει την σύσταση που κάναμε στο προηγούμενο κεφάλαιο, δηλαδή πρώτα να γίνεται η συλλογή και το φιλτράρισμα και στη συνέχεια η ανάλυση. Επομένως εμφανίζουμε όλες τις συνδέσεις, καταγράφουμε τα αποτελέσματα σε αρχείο και στη συνέχεια αναζητούμε τα αποτελέσματα για τις καταχωρήσεις που μας ενδιαφέρουν.

Τα περισσότερα sniffer εμπορικής χρήσης έχουν δυνατότητες φιλτραρίσματος και εμφανίζουν μόνο τα πακέτα που ταιριάζουν με τα κριτήρια αναζήτησης. Εναλλακτικά, μπορούμε να κατατάξουμε τους υπολογιστές προορισμού βάσει του όγκου των δεδομένων που στάλθηκαν και λήφθηκαν. Με αυτόν τον τρόπο μπορεί να αποκαλυφθεί ένα υπολογιστικό σύστημα το οποίο εμπλεκόταν σε μεγάλο όγκο μεταφοράς δεδομένων. Παρόμοια μπορεί να γίνει κατάταξη βάσει των συνδέσεων μεταξύ των υπολογιστικών συστημάτων, που μπορεί οδηγήσει σε χρήσιμα συμπεράσματα κατά την ανάλυση της δικτυακής κίνησης. Ένα εργαλείο που μπορεί να μας βοηθήσει είναι το NetIntercept με τις αναφορές "Traffic Load" και "Top N".

2.4.5 Χαρακτηριστικά κλάσης και επιβεβαίωση πηγής

Καθώς τα δίκτυα εξελίσσονται, περιέχουν έναν ολοένα αυξανόμενο αριθμό διαφορετικών τύπων δεδομένων κάνοντας δύσκολη την αναγνώρισή τους. Βέβαια, όπως και στις υπόλοιπες μορφές ψηφιακών αποδεικτικών στοιχείων, τα χαρακτηριστικά κλάσης μπορούν να χρησιμοποιηθούν για να διαφοροποιήσουν τις ιστοσελίδες από τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα αρχεία καταγραφής των διακομιστών ιστού από τα αρχεία καταγραφής των διακομιστών e-mail. Επιπλέον τα χαρακτηριστικά κλάσης μπορούν να αποκαλύψουν πιο πρόγραμμα χρησιμοποιήθηκε για να δημιουργήσει ένα δεδομένο στοιχείο των ψηφιακών αποδεικτικών στοιχείων καθώς και το λειτουργικό σύστημα στο οποίο δημιουργήθηκε. Ακόμη τα ψηφιακά αποδεικτικά στοιχεία στα δίκτυα μπορεί να περιλαμβάνουν χαρακτηριστικά όπως τις διευθύνσεις IP και MAC, οι οποίες σε μερικές περιπτώσεις αποτελούν μοναδικά χαρακτηριστικά. Επομένως τα χαρακτηριστικά αυτά μπορούν να επιβεβαιώσουν την πηγή των αποδεικτικών στοιχείων στο δίκτυο.

Τα αρχεία κεφαλίδας στα μηνύματα e-mail προσδίδουν αυτά τα χαρακτηριστικά κλάσης και μοναδικότητας και επαληθεύουν την πηγή των δικτυακών δεδομένων. Η ακόλουθη κεφαλίδα προσδιορίζει ότι το μήνυμα στάλθηκε από ένα σύστημα με λειτουργικό Mandrake Linux με επεξεργαστή Intel 586 που εκτελεί το X11 και ένα πρόγραμμα πελάτη ηλεκτρονικού ταχυδρομείου που εκτελείται στον Mozilla v. 4.75. Εάν έχει ανατεθεί στον υπολογιστή η διεύθυνση IP 192.168.187.18 τότε ο υπολογιστής μπορεί να εντοπιστεί και τα χαρακτηριστικά κλάσης μπορούν να χρησιμοποιηθούν ούτως ώστε να επιβεβαιώσουν τη σύνδεση με τον υπολογιστή.

Return-Path; <harasser@threat.net>

Received: from attack.threat.net (attack.threat.net [192.168.187.18])
by lsh110.siteprotect.com (8.9.3/8.9.3) with SMTP id MAA21755
for <eco@corpus-delicti.com>; Wed, 29 Jan 2003 12:38:30 -0600

To: eco@corpus-delicti.com

Date: Wed, 29 Jan 2003 13:32:19 -0500

Message-ID: <1043865139.9860@attack.threat.net>

X-Mailer: Mozilla 4.75 [en] (X11; U; Linux 2.2.17-21 mdk i586)

From: harasser@threat.net

Subject: Your Worst Nightmare!

Αυτά τα χαρακτηριστικά μπορούν να χρησιμοποιηθούν για να αναζητήσουμε στο διαδίκτυο ή στον υπολογιστή ενός υπόπτου για μηνύματα με τα ίδια χαρακτηριστικά. Επιπλέον όταν ένας υπάλληλος στοχεύει έναν άλλο υπάλληλο του οργανισμού, τότε τα συστήματα υπολογιστών στο δίκτυο του οργανισμού μπορεί να περιέχουν σχετικά ψηφιακά αποδεικτικά στοιχεία.

Οι καταχωρήσεις σε ένα αρχείο καταγραφής πρόσβασης σε ένα διακομιστή ιστού παρέχει και άλλα παραδείγματα χαρακτηριστικών των κλάσεων και επιβεβαίωσης της πηγής των δικτυακών δεδομένων. Η ακόλουθη καταχώρηση ενός αρχείου καταγραφής δείχνει ότι η ιστοσελίδα "project.html" προσπελάστηκε από την διεύθυνση IP 172.16.1.19 χρησιμοποιώντας το περιηγητή ιστού Mozilla έκδοσης 4.75, προσαρμοσμένο στα αγγλικά, και έναν υπολογιστή με λειτουργικό σύστημα Windows 2000.

2003-01-23 12:52:40 172.16.1.19 - 192.168.1.3 80 GET /documents/ project21.html - 200 Mozilla/4.75+[en]+(Windows+NT+5.0;+U)

Αυτά τα χαρακτηριστικά κλάσης όπως ο περιηγητής ιστού και ο τύπος του μηχανήματος μπορούν να παραποιηθούν κατά την αίτηση προς τον διακομιστή ιστού. Οι ακόλουθες καταχωρήσεις του αρχείου καταγραφής από τον ίδιο διακομιστή ιστού δείχνουν μία απόπειρα παρείσφρησης μέσω μίας γνωστής ευπάθειας στον Internet Information Server (IIS) της Microsoft. Οι διαφοροποιήσεις στην έκδοση του περιηγητή ιστού και στον τύπο του συστήματος που σχετίζονται με μία μοναδική διεύθυνση IP υποδεικνύει ότι αυτή η πληροφορία είναι κατασκευασμένη. Αν και τα χαρακτηριστικά κλάσης αποκαλύπτουν ιδιότητες του συστήματος του επιτιθέμενου, μπορεί επίσης να αποκαλύψουν και το πρόγραμμα που χρησιμοποιήθηκε για την εκτέλεση της επίθεσης. Συγκρίνοντας τα χαρακτηριστικά κλάσης με αυτά άλλων προγραμμάτων εκμετάλλευσης ευπαθειών μπορεί να μας

οδηγήσουν σε ταύτιση. Η ταύτιση αυτή μπορεί να είναι με μία έκδοση του σκουληκιού Nimda ή σε περίπτωση που η επίθεση πραγματοποιήθηκε από ένα μόνο άτομο, αυτή η πληροφορία μπορεί να χρησιμοποιηθεί για να διερευνηθεί το σύστημα του υπαίτιου ώστε να ανακαλύψουμε το εργαλείο που χρησιμοποίησε.

2003-01-23 12:59:02 137.56.97.25 - 192.168.1.3 80 HEAD
/winnt/system32/cmd.exe /c+dir+c:/ 403
Mozilla/4.0+(+compatible;+[fr];+Windows+NT5.0;+athome020+)
2003-01-23 12:59:02 137.56.97.25 - 192.168.1.3 80 HEAD /cgi-
bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe /c+dir+c:/ 403
Mozilla/4.7+(+compatible;+MSIE+5.0;+AOL+5.0;+DigiExt+)
2003-01-23 12:59:02 137.56.97.25 - 192.168.1.3 80 HEAD
/msadc/..%2f..%2f..%2f..%2fwinnt/system32/cmd.exe /c+dir+c:/ 500
Mozilla/4.0+(+compatible;+[fr];+Windows+NT5.0;+DigiExt+)
2003-01-23 12:59:02 137.56.97.25 - 192.168.1.3 80 HEAD
/msadc/..?/€/?/€/?/€/?../winnt/system32/cmd.exe /c/+dir+c:/ 404
Mozilla/4.7+(+compatible;+MSIE+5.0;+Windows+NT5.0;+Compaq+)

Τα αποτελέσματα της υπερχείλισης του ενταμιευτή σε ένα σύστημα αποτελούν ένα ακόμη παράδειγμα των χαρακτηριστικών κλάσης και επιβεβαίωσης της πηγής σε ένα δίκτυο. Η υπερχείλιση του ενταμιευτή είναι συνηθισμένος τρόπος παρείσφρησης σε συστήματα υπολογιστών. Όταν ένα πρόγραμμα αποτυγχάνει να περιορίσει το μήκος της τιμής εισόδου, τότε μπορούμε να δώσουμε μεγαλύτερη τιμή εισόδου από αυτήν που περιμένει, γεγονός που έχει ως αποτέλεσμα την εγγραφή της υπόλοιπης πληροφορίας στη μνήμη του υπολογιστή. Με προσεκτική δημιουργία αυτής της μεγάλης τιμής εισόδου, μπορεί να γίνει εκμετάλλευση αυτής της αδυναμίας του προγράμματος, με αποτέλεσμα την εκτέλεση εντολών στον υπολογιστή και ο εισβολέας να αποκτήσει δικαίωμα προσπέλασης στο σύστημα. Για παράδειγμα, στην παρακάτω εικόνα παρουσιάζεται το κομμάτι ενός αρχείου καταγραφής που ανακτήθηκε από ένα παραβιασμένο σύστημα. Βλέπουμε ότι η διεύθυνση IP του επιτιθέμενου είναι 192.168.1.231 και αξιοποιήθηκε μία ευπάθεια στον διακομιστή FTP.

```
Jan 24 17:07:22 target ftpd[567]: FTP session closed
Jan 25 00:21:54 target ftpd[576]: ANONYMOUS FTP LOGIN FROM
attacker.corpX.com [192.168.1.231],
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□1À1Û1É°FÍ□1À1ÛC‰ÙA
°?Í□ëk^1À1É□^^A^F^Df¹ÿ^A°'Í□1À□^^A°=Í□1À1Û□^^H‰C^B1ÉþÉ1À□^^H°^LÍ□þÉuó1À^F
^I□^^H°=Í□þ^N°0þÈ^F^D1À^F^G‰v^H‰F^L‰ó□N^H□V^L°^KÍ□1À1Û°^AÍ□è□ÿÿÿ0bin0sh1.
.11
Jan 24 17:22:54 target inetd[448]: pid 576: exit status 1
```

Αν οι εισβολείς χρησιμοποιήσουν πλαστές διευθύνσεις IP κατά την αποστολή των πακέτων, τότε δεν χρειάζονται απάντηση από το σύστημα στόχο, αλλά στην περίπτωση του παραδείγματος μας δεν μπορεί να γίνει πλαστογράφηση της διεύθυνσης καθώς η ευπάθεια χρησιμοποιεί το TCP ώστε να επιστραφεί στον εισβολέα γραμμή εντολών. Η διερεύνηση σε αρχεία καταγραφής συστημάτων ανίχνευσης παρείσφρησης για την διεύθυνση IP, μπορεί να αποκαλύψει άλλες απόπειρες παρείσφρησης. Εξετάζοντας άλλα συστήματα για διαγραμμένα κομμάτια αρχείων καταγραφής παρόμοια με αυτό που βρέθηκε, μπορεί να βοηθήσει στην αναγνώριση άλλων συστημάτων που παραβιάστηκαν. Επιπλέον, εάν βρεθεί ο προσωπικός υπολογιστής του εισβολέα και βρεθεί ένα πρόγραμμα για την εκμετάλλευση των διακομιστών FTP τότε μπορεί να γίνει σύγκριση και να καθοριστεί εάν υπάρχει συνέπεια με το παραπάνω αρχείο καταγραφής.

Χρήσιμα χαρακτηριστικά κλάσης μπορούν επίσης να εντοπιστούν στην κίνηση δικτύου μέσω του πρωτοκόλλου TCP/IP. Στην πραγματικότητα τα συστήματα ανίχνευσης παρείσφρησης βάσει υπογραφών, εξαρτώνται από χαρακτηριστικά της κίνησης δικτύου για να κατηγοριοποιήσουν τις επιθέσεις. Για παράδειγμα, το εργαλείο Snort ανιχνεύει επιτυχείς επιθέσεις κατά των διακομιστών IIS αναζητώντας πακέτα από την θύρα 80 που περιλαμβάνουν τον όρο "Volume Serial Number" υποδηλώνοντας επιτυχή προσπέλαση στον κατάλογο του ευπαθούς διακομιστή ιστού. Η προειδοποίηση που δίνει ως αποτέλεσμα το σύστημα ανίχνευσης παρείσφρησης περιλαμβάνει την ημερομηνία, την ώρα, τις διευθύνσεις IP καθώς και άλλες πληροφορίες σχετικές με το πακέτο.

[**] [1:1292:1] ATTACK RESPONSES http dir listing [**]

01/23-12:59:02.865832 192.168.1.3:80 -> 137.56.97.25:25587

TCP TTL:127 TOS:0x0 ID:8817 IpLen:20 DgmLen:243 DF

****AP*** Seq: 0x5E3A36C3 Ack: 0x58C4137F Win: 0x4313 TcpLen: 32*

TCP Options (3) => NOP NOP TS: 16339694 242252

Το δημοφιλές πρόγραμμα σάρωσης θυρών που ονομάζεται nmap χρησιμοποιεί τα χαρακτηριστικά κλάσης των πακέτων TCP/IP που επιστρέφονται από το τερματικό σύστημα για να καθοριστεί το απομακρυσμένο λειτουργικό σύστημα.

C:\> nmap -sS -PT -PI -O -T 3 192.168.0.2

Starting nmap V. 3.00 (www.insecure.org/nmap)

Interesting ports on HOST101 (192.168.0.2):

(The 1600 ports scanned but not shown below are in state: closed)

Port	*State*	*Service*
139/tcp	*open*	*netbios-ssn*

Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP

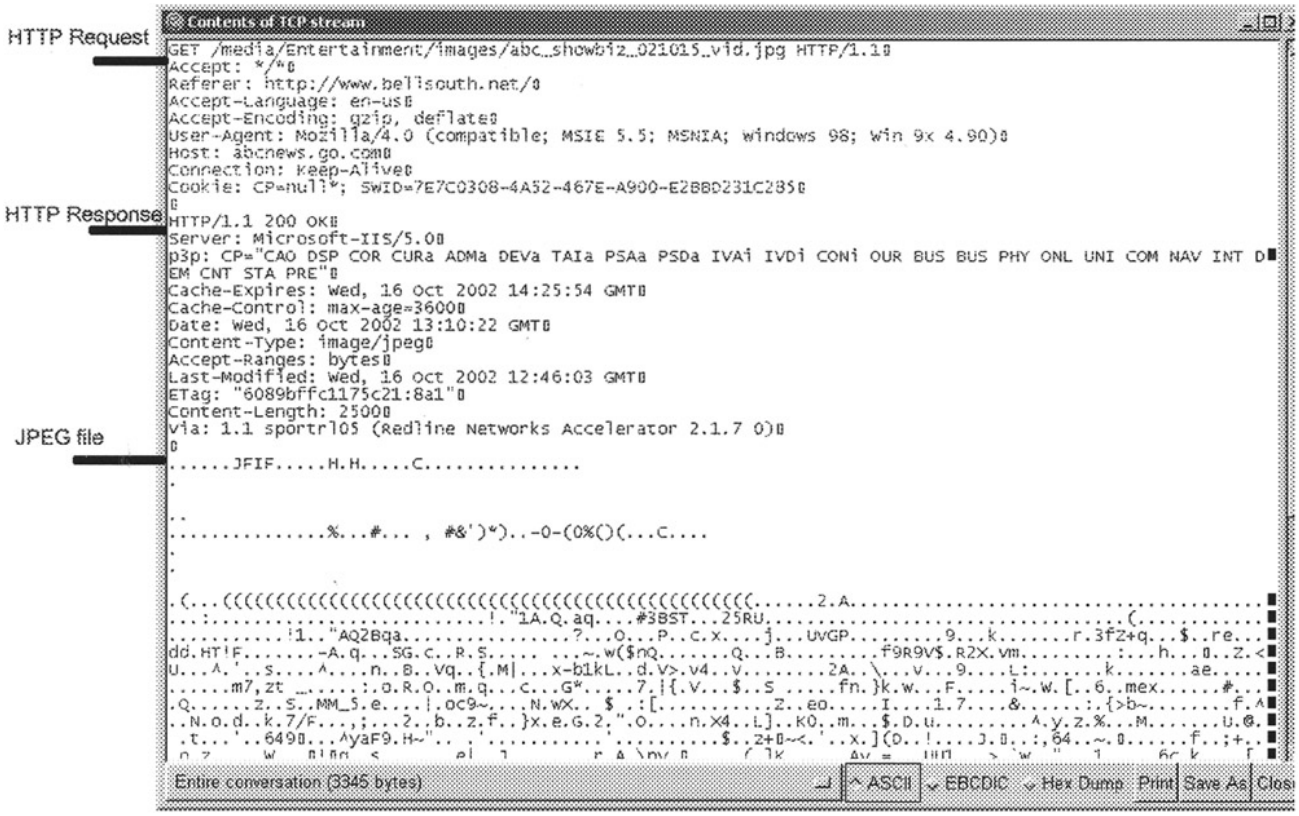
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds

Οι ψηφιακοί ερευνητές μπορούν επίσης να χρησιμοποιήσουν τα χαρακτηριστικά κλάσης ώστε να έχουν καλύτερη γνώση σχετικά με ασυνήθιστα πακέτα τα οποία έχουν δημιουργηθεί με μοναδικό σκοπό να είναι επιβλαβή στα υπολογιστικά συστήματα. Η διαφοροποίηση αυτών των πακέτων σε σχέση με τα κανονικά πακέτα μπορεί να βοηθήσει τους ερευνητές στην καλύτερη κατανόηση των συμβάντων. Ακόμη τα χαρακτηριστικά των πακέτων μπορούν να καθορίσουν το εργαλείο που χρησιμοποιήθηκε. Εάν ένα πακέτο ίδιου τύπου, χρησιμοποιήθηκε για την εισβολή σε διάφορους διακομιστές ιστού ενός οργανισμού, είναι πολύ πιθανό ότι ένα άτομο είναι υπεύθυνο για όλα τα περιστατικά. Επομένως γνωρίζοντας ότι υπάρχει μόνο ένας υπαίτιος για την επίθεση στους διακομιστές ιστού, μπορεί να βοηθηθούμε ώστε να αποκαλύψουμε τα κινήτρα του υπαίτιου.

2.4.6 Ανάκτηση ψηφιακών αποδεικτικών στοιχείων

Η ανάκτηση των ψηφιακών αποδεικτικών στοιχείων όπως τα αρχεία καταγραφής συστήματος ή δικτύου από ένα διακομιστή αφορούν τεχνικές της ψηφιακής δικανικής. Μπορούν να εντοπιστούν διαγραμμένα κομμάτια αρχείων καταγραφής συστήματος στον αδιάθετο χώρο, αναζητώντας για χαρακτηριστικά όπως ημερομηνία ή πεδία μηνύματος. Ακόμη μπορεί να είναι δυνατό να επιδιορθωθούν τα κατεστραμμένα αρχεία καταγραφής "wtmp" του UNIX ή τα αρχεία καταγραφής NT Event ή τουλάχιστον να εξαχθούν κάποιες χρήσιμες πληροφορίες από τα μη κατεστραμμένα κομμάτια. Να σημειώσουμε ότι ένα αρχείο "wtmp" είναι δυνατό να καταστραφεί με τρόπο που δεν είναι προφανής και όταν γίνει η επεξεργασία του μπορεί να συσχετιστεί με λάθος χρήστη με λάθος τρόπο σύνδεσης. Με αυτό το παράδειγμα υποδηλώνεται η σημαντικότητα της επιβεβαίωσης των σημαντικών αρχείων καταγραφής πριν τα χρησιμοποιήσουμε για να οδηγηθούμε σε ασφαλή συμπεράσματα.

Επίσης είναι δυνατή η ανάκτηση των ψηφιακών αποδεικτικών στοιχείων από την κίνηση δικτύου. Η δικτυακή κίνηση που σχετίζεται με μία συσκευή μπορεί να περιλαμβάνει επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, κατεβασμένα αρχεία, ιστοσελίδες, και ακόμη περισσότερα. Κατά την ανάκτηση της δικτυακής κίνησης μπορούν να προκύψουν ενδιαφέροντα στοιχεία, εάν εξάγουμε ξεχωριστά πακέτα και στη συνέχεια τα συνδυάσουμε. Για παράδειγμα στην παρακάτω εικόνα παρουσιάζεται ένα δικτυακό sniffer το οποίο ονομάζεται Ethereal και χρησιμοποιείται για να αναδημιουργήσει μία ροή TCP και να παρουσιάσει τα περιεχόμενα από την επικοινωνία. Στο παράδειγμα αυτό έγινε αίτημα για σύνδεση για μία εικόνα JPEG από τον διακομιστή ιστού. Κατά τη διαδικασία της αναδημιουργίας το Ethereal συλλέγει δεδομένα από το φυσικό επίπεδο, εξάγοντας μόνο τα σχετικά πακέτα από το επίπεδο μεταφοράς και το επίπεδο δικτύου, και παρουσιάζει το πρωτόκολλο επιπέδου εφαρμογής, δηλαδή ένα αίτημα HTTP GET για μία εικόνα σε μία ιστοσελίδα.



Εικόνα 4: Στιγμιότυπο του Ethereal που χρησιμοποιείται για να αναδημιουργήσει μία ροή TCP που σχετίζεται με ένα συστατικό μιας ιστοσελίδας καθώς αυτή κατεβαίνει (Casey, 2004).

Το Ethereal δεν σχεδιάστηκε με γνώμονα τη συλλογή ψηφιακών αποδεικτικών στοιχείων αλλά παραμένει χρήσιμο για τη διερεύνηση της δικτυακής κίνησης. Το Ethereal έχει δυνατότητα αποθήκευσης των δεδομένων σε αρχείο και στη συνέχεια την προβολή τους μέσω του κατάλληλου προγράμματος όπως ένα περιηγητή ιστού. Ωστόσο το παραγόμενο αρχείο περιέχει συχνά δεδομένα που αποτρέπει άλλα προγράμματα να παρουσιάσουν σωστά το αρχείο. Με αυτόν τον τρόπο έχουμε την αίσθηση ότι εγκαθιδρύθηκε η επικοινωνία αλλά δεν παρουσιάζονται τα δεδομένα όπως τα είδε ο χρήστης.

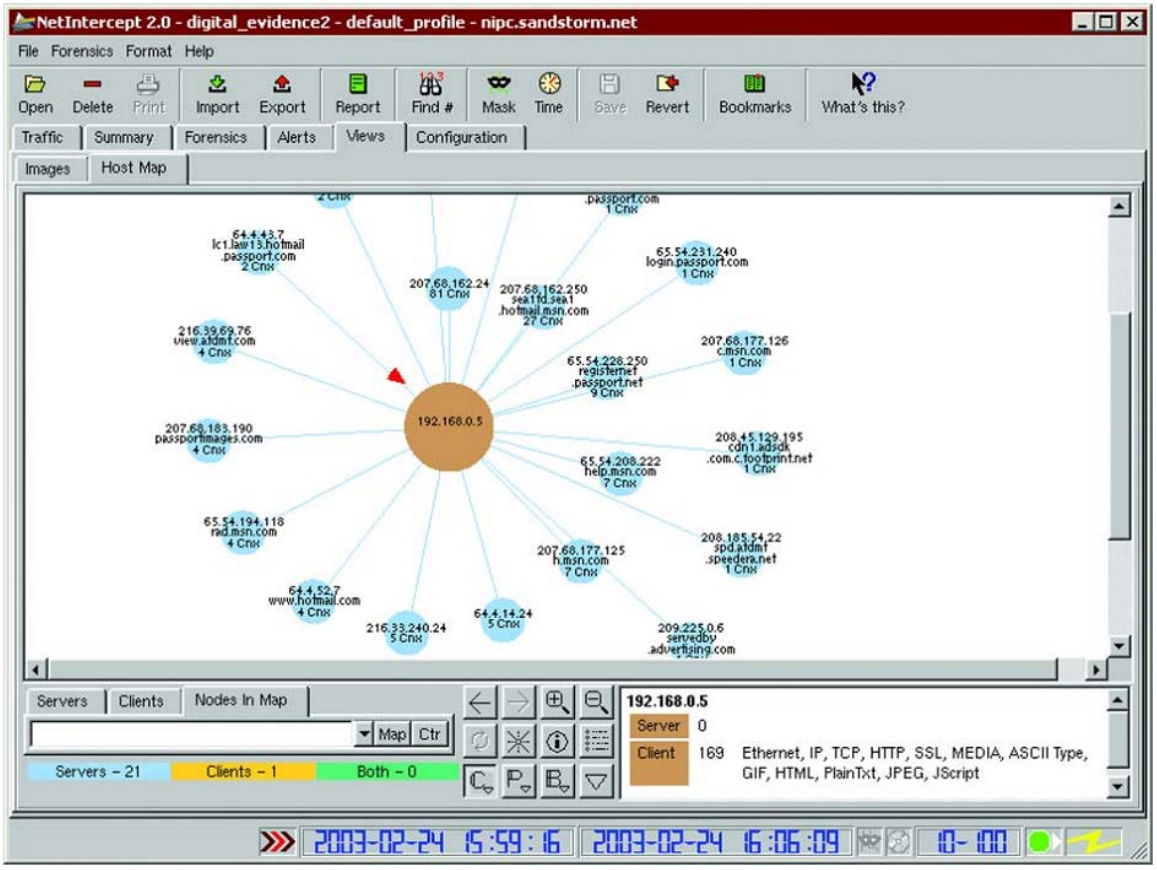
Άλλα εργαλεία διερεύνησης δικτύων μπορούν να αναδημιουργήσουν και να παρουσιάσουν αποτελεσματικότερα τα αρχεία από πακέτα κίνησης δικτύου. Για παράδειγμα το εργαλείο NetIntercept παρέχει μια οργανωμένη άποψη των εικόνων που ανακτήθηκαν από το δίκτυο ώστε να είναι αποδοτικότερο για τους ψηφιακούς ερευνητές. Ακόμη το NetIntercept και άλλα παρόμοια εργαλεία μπορούν να αναδημιουργήσουν ιστοσελίδες, επιτρέποντάς στους ερευνητές να δούνε τις ιστοσελίδες όπως τις είδε ο χρήστης. Διαφορετικά εργαλεία ανάλυσης δικτύου μπορούν να

αναδημιουργήσουν και να παρουσιάσουν διαφορετικούς τύπους δεδομένων όπως μηνύματα ηλεκτρονικού ταχυδρομείου, FTP, μηνύματα άμεσης απάντησης με διαφορετικό πάντα βαθμό επιτυχίας. Οπότε όταν ένας τρίτος κατεβάζει ένα συμπιεσμένο αρχείο μέσω ενός διακομιστή FTP ή μέσω του IRC είναι θεμιτό να ανακτήσουμε το αρχείο συλλαμβάνοντας το στο δίκτυο και εξετάζοντας τα περιεχόμενα του. Ορισμένες μορφοποιήσεις δεδομένων παρουσιάζουν μεγαλύτερη δυσκολία κατά την ανάκτησή τους και απαιτούν τη χρήση εργαλείων ειδικού σκοπού.

Ανεξάρτητα από τα εργαλεία που χρησιμοποιούνται κατά τη συλλογή και την ανάλυση της δικτυακής κίνησης στα συστήματα αυτά, οι ψηφιακοί ερευνητές πρέπει να λάβουν επιπλέον ενέργειες και να τεκμηριώσουν επιπλέον στοιχεία που δεν καταγράφηκαν από τα εργαλεία, όπως τη τιμή συνόψισης MD5 των αρχείων tcpdump τα οποία περιέχουν τη δικτυακή κίνηση, τον αριθμό των πακέτων που χάθηκαν και τις ενέργειες που εκτέλεσε ο ερευνητής κατά την ανάλυση των δεδομένων.

2.4.7 Αναδημιουργία της διαδικασίας διερεύνησης δικτύων

Θα παραθέσουμε κάποια παραδείγματα που θα βοηθήσουν στην κατανόηση της αναδημιουργίας της διαδικασίας διερεύνησης δικτύων. Για παράδειγμα, στην παρακάτω εικόνα η δικτυακή κίνηση αναπαρίσταται με συνδέσεις σημείο προς σημείο και δίνεται έμφαση στο τερματικό σύστημα που παρουσιάζει τη μεγαλύτερη δραστηριότητα και αξίζει περαιτέρω διερεύνησης.



Εικόνα 5: Αποτύπωση με τη χρήση του εργαλείου NetIntercept της κίνησης δικτύου βάσει των διασυνδεδεμένων διευθύνσεων IP (Casey, 2004).

Η δημιουργία διαγράμματος συνδέσεων που παρουσιάζει τις συνδέσεις πελάτη διακομιστή μπορεί να βοηθήσει στην αναγνώριση σημαντικών συστημάτων. Για παράδειγμα κατά τη διερεύνηση παρείσφρησης υπολογιστικών συστημάτων, η επικέντρωση της έρευνας στην διεύθυνση IP του επιτιθέμενου μπορεί να αποκαλύψει τα τερματικά συστήματα τα οποία είχε ως στόχο και στη συνέχεια εξετάζεται η κίνηση από κάθε στόχο που μας δείχνει ποια συστήματα παραβιάστηκαν. Η εξέταση της κίνησης από ένα εκτεθειμένο σύστημα μπορεί να δώσει στους ερευνητές μία γενική αίσθηση των ενεργειών που εκτέλεσε ο επιτιθέμενος.

Ωστόσο η διαδικασία της αναδημιουργίας αποτελεί πρόκληση καθώς εμπλέκονται δίκτυα. Ο εγκληματίας ή το θύμα μπορεί να βρίσκονται σε κάθε δεδομένη χρονική στιγμή σε διαφορετικά σημεία σε ένα δίκτυο με αποτέλεσμα η διαδικασία αναδημιουργίας να εξελίσσεται σε επίπονη και πολύπλοκη διαδικασία.

Ο υπαίτιος μπορεί να χρησιμοποιήσει το διαδίκτυο για να αποκρύψει την πραγματική τοποθεσία του και να συνδεθεί διαμέσου υπολογιστών σε άλλα μέρη στην χώρα ή στον κόσμο. Οι εισβολείς υπολογιστικών συστημάτων χρησιμοποιούν αυτή την τεχνική ξεκινώντας την επίθεση τους από ένα εκτεθειμένο σύστημα σε μία απομακρυσμένη περιοχή ώστε να αποκρύψουν την διεύθυνση IP και την τοποθεσία τους. Επίσης τα εικονικά δίκτυα (VPN) επεκτείνουν με ασφάλεια το δίκτυο τοπικής περιοχής σε οποιοδήποτε μέρος του κόσμου, παρέχοντας μία κρυπτογραφημένη σύνοδο μεταξύ ενός υπολογιστή σε μία απομακρυσμένη περιοχή με το τοπικό δίκτυο.

Το έργο της διερεύνησης γίνεται δυσκολότερο καθώς οι υπολογιστές μπορεί να μετακινούνται, να τους ανατίθενται νέες διευθύνσεις IP, να αλλάζουν οι καταχωρήσεις DNS, να γίνεται σύνδεση με ένα υπολογιστικό σύστημα εξ αποστάσεως ή μέσω ενός αριθμού συστημάτων. Επομένως προτού γίνει η υπόθεση ότι με βάση την διεύθυνση IP ένα άτομο βρισκόταν σε μία συγκεκριμένη τοποθεσία ή ο υπολογιστής βρισκόταν σε μία συγκεκριμένη τοποθεσία, θα πρέπει να εξεταστούν ενδελεχώς οι εναλλακτικές περιπτώσεις. Επιπλέον θα πρέπει να είμαστε προσεκτικοί στις υποθέσεις που κάνουμε από μία καταχώρηση ενός αρχείου καταγραφής. Μία καταγεγραμμένη προσπάθεια σύνδεσης στα αρχεία καταγραφής δικτύου δε σημαίνει απαραίτητα ότι προσπελάστηκε το σύστημα. Ακόμη χρειάζονται επιβεβαιωμένα δεδομένα που να καθορίζουν ότι ένας τρίτος προσπέλασε το σύστημα με επιτυχία. Μία ανάλυση λειτουργιών μπορεί να αποκαλύψει ότι το σύστημα είχε ρυθμιστεί ώστε να αποτρέπει τέτοιου είδους πρόσβαση.

Παρακάτω θα δώσουμε ένα παράδειγμα που περιλαμβάνει ένα διακομιστή Linux που παραβιάστηκε μέσω FTP και αποδεικνύει την αξία της επιβεβαίωσης της πηγής των αποδεικτικών στοιχείων σε ένα δίκτυο.

Ανάλυση περίπτωσης:

Μία παρείσφρηση σε ένα υπολογιστικό σύστημα ανιχνεύθηκε γρήγορα χρησιμοποιώντας το λογισμικό Tripwire, όταν διάφορα συστατικά του συστήματος αντικαταστάθηκαν με ένα rootkit. Η ακόλουθη καταχώριση στο φάκελο /var/log/secure έδειξε ότι πραγματοποιήθηκε σύνδεση με τον διακομιστή FTP.

Apr 24 22:50:34 ftpserver in.ftpd[2103]: connect from 62.30.247.138

Η καταχώριση που αποτέλεσε απόκριση της προηγούμενης ενέργειας είναι η παρακάτω:

ftp ftp pc-62-30-247-138-do.blueyonder.co.uk [62.30.247.138] Tue Apr 24 22:50-22:50 (00:00)

Αυτή η μη εξουσιοδοτημένη σύνδεση υποστηρίχθηκε εν μέρει από την ακόλουθη καταχώριση στο φάκελο /var/log/messages, όπου η μόνη διαφορά είναι το χρονικό σημείο που έγινε:

Apr 25 02:50:40 ftpserver ftpd[2103]: ANONYMOUS FTP LOGIN FROM pc-62-30-247-138-do.blueyonder.co.uk [62.30.247.138], guest@here.com

Με δεδομένο ότι μπορεί να έχουν μεταβληθεί τα αρχεία καταγραφής στο παραβιασμένο τερματικό σύστημα, οι ψηφιακοί ερευνητές πραγματοποίησαν έλεγχο στα αρχεία καταγραφής του συστήματος αναγνώρισης παρείσφρησης για μια αντίστοιχη καταχώρηση αλλά χωρίς επιτυχία. Ωστόσο βρήκαν μία καταχώρηση με διαφορετική ημερομηνία και πηγή.

[**] FTP-site-exec [**]
04/25-02:48:44 04/25-02:49:37 63 62.122.10.221 -> 192.168.2.6S: 4158 D: 21

Για να έχουν μία πληρέστερη εικόνα των πραγματικών γεγονότων, οι ψηφιακοί ερευνητές αναζήτησαν τα αρχεία καταγραφής NetFlow για να δουν όλες τις συνδέσεις από και προς το παραβιασμένο σύστημα. Ανακάλυψαν ότι η αρχική σύνδεση από το blueyonder.co.uk στις 22:50:34 ήταν κομμάτι μίας ευρύτερης διερεύνησης για διακομιστές FTP, οι οποίοι δεν καταγράφηκαν από το σύστημα ανίχνευσης παρείσφρησης. Τα αρχεία καταγραφής του NetFlow έδειξαν ότι η πραγματική εισβολή πραγματοποιήθηκε στις 02:47:12 από το 62-122-10-221.flat.galactica και ο εισβολέας κατέβασε ένα διορθωτικό πακέτο λογισμικού από το RPMfind.net για να διορθώσει την ευπάθεια. Αυτή είναι συνήθης πρακτική των εισβολέων ούτως ώστε να αποτρέψουν άλλους εισβολείς να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα και να αποκρύψουν το γεγονός ότι παραβιάστηκε το σύστημα.

Γενικότερα θα πρέπει να γίνει ανάλυση σε όλα τα διαθέσιμα αρχεία καταγραφής ώστε να

αναγνωριστούν τα κρίσιμα σημεία σε ένα έγκλημα. Τα αρχεία καταγραφής των δρομολογητών, τα τείχη προστασίας, τα συστήματα ανίχνευσης παρείσφρησης αλλά και άλλες πηγές εάν συνδυαστούν, μπορούν να μας οδηγήσουν σε σημαντικά στοιχεία. Για παράδειγμα όταν ένας εισβολέας στοχεύει συστήματα σε ένα δίκτυο τα αρχεία καταγραφής; του τείχους προστασίας μπορεί να έχουν καταγράψει μόνο ορισμένες αποτυχημένες προσπάθειες σύνδεσης που δεν ήταν ανησυχητικές. Ωστόσο εάν συνδυαστούν με τα αρχεία καταγραφής των δρομολογητών και των συστημάτων ανίχνευσης παρείσφρησης μπορεί να γίνει εμφανές ότι οι αποτυχημένες προσπάθειες σύνδεσης ήταν μέρος μίας εκτεταμένης σειράς επιθέσεων εναντίον πολλών συστημάτων στο δίκτυο. Όταν εκτελούμε ανάλυση σε πολλαπλά αρχεία καταγραφής είναι περισσότερο αποτελεσματικό να τα συνδυάσουμε πριν τα ταξινομήσουμε και τα αναλύσουμε.

2.5. Διερεύνηση δικτύων στο φυσικό επίπεδο δικτύωσης και επίπεδο ζεύξης

Η συνηθέστερη προσέγγιση για τη συλλογή ψηφιακών αποδεικτικών στοιχείων στο φυσικό επίπεδο δικτύωσης είναι η χρησιμοποίηση ενός sniffer. Τα sniffer εξαναγκάζονται να παρακολουθούν όλη την κίνηση που πραγματοποιείται στο δίκτυο. Δεδομένου ότι οι μεταγωγείς αποτρέπουν σε ένα τερματικό σύστημα να παρακολουθεί την κίνηση στα άλλα τερματικά συστήματα στο δίκτυο, οι εισβολείς παρακολουθούν συνήθως μόνο την κίνηση από και προς το υπολογιστικό σύστημα που παραβίασαν. Ορισμένοι επιτιθέμενοι καταγράφουν την δικτυακή κίνηση τους χρησιμοποιώντας sniffer και στη συνέχεια ελέγχουν την καταγεγραμμένη κίνηση.

Άλλοι εγκληματίες λαμβάνουν μέτρα ενάντια στις υποκλοπές χρησιμοποιώντας κρυπτογράφηση. Είναι πρακτικά αδύνατο να σπάσουμε μία ισχυρή κρυπτογράφηση. Για παράδειγμα, οι εισβολείς που γνωρίζουν ότι οι ερευνητές μπορεί να παρακολουθούν τις συνόδους τους θα τις κρυπτογραφήσουν με λογισμικό όπως το SSH. Ωστόσο, ακόμα και εάν τα δεδομένα είναι κρυπτογραφημένα η συλλογή και ανάλυση της δικτυακής κίνησης μπορεί να μας δώσει πληροφορίες. Εάν για παράδειγμα, διακινούνται εκατοντάδες πακέτα με κρυπτογραφημένα δεδομένα μεταξύ δύο προσώπων ενώ ο ένας εκ των δύο διέπραξε έγκλημα, τότε το δεύτερο άτομο μπορεί να θεωρηθεί ως συνεργός, γεγονός που μπορεί να αποτελέσει αιτία για τη διερεύνηση του υπολογιστικού συστήματός του.

Τα sniffers μπορούν να χρησιμοποιηθούν με διαφορετικούς τρόπους σε ένα δίκτυο. Μετά τη μη

εξουσιοδοτημένη προσπέλαση ενός επιτιθέμενου σε ένα τερματικό σύστημα Linux, οι ψηφιακοί ερευνητές μπορούν να χρησιμοποιήσουν το tcpdump στο σύστημα που παραβιάστηκε ώστε να καταγράψουν τη δικτυακή κίνηση από και προς το παραβιασμένο τερματικό σύστημα. Ωστόσο, χρησιμοποιώντας το παραβιασμένο σύστημα για τη συλλογή ψηφιακών αποδεικτικών στοιχείων μπορεί να καταστραφούν άλλα χρήσιμα αποδεικτικά στοιχεία. Επιπλέον ο εισβολέας μπορεί να τροποποίησε το λογισμικό tcpdump για να αποκαλύψει ή για να αποκρύψει τα ψηφιακά αποδεικτικά στοιχεία. Αντί αυτού οι ερευνητές μπορούν να χρησιμοποιήσουν ένα γειτονικό τερματικό σύστημα στο ίδιο κομμάτι δικτύου ώστε να παρακολουθήσουν την κίνηση από και προς το παραβιασμένο σύστημα. Βέβαια η προσέγγιση αυτή της συλλογής της κίνησης δικτύου ως αποδεικτικό στοιχείο, είναι αποτελεσματική μόνο όταν οι υπολογιστές είναι συνδεδεμένοι σε έναν ομφαλό.

Κατά την ανάλυση της κίνησης δικτύου είναι θεμιτό να γνωρίζουμε τα συμβάντα χρόνου που προέκυψαν. Η μορφοποίηση του tcpdump περιλαμβάνει την ημερομηνία και ώρα για το κάθε πλαίσιο που καταγράφηκε αλλά ορισμένα εργαλεία συμπεριλαμβανομένου του tcpdump παρουσιάζουν μόνο την ώρα και όχι την ημερομηνία. Για παράδειγμα, χρησιμοποιώντας το tcpdump για να δούμε το αρχείο με όνομα hotmail-02242003.dmp δεν περιλαμβάνεται η ημερομηνία αλλά μόνο ο χρόνος.

```
examiner1% tcpdump -r hotmail-02242003.dmp
15:59:15.501154 192.168.0.5.32769 > 192.168.0.1.53: 6342+ A?
www.hotmail.com. (33) (DF)
```

Εξετάζοντας το ίδιο αρχείο tcpdump παρατηρούμε μία τιμή ημερομηνίας και ώρας A3875A3E που ισοδυναμεί με τη Δευτέρα 24 Φεβρουαρίου 2003 και ώρα 15:59:15 GMT-0500.

Κατά τη διάρκεια μίας διερεύνησης είναι συχνά χρήσιμο να αναζητούμε στο αρχείο tcpdump μία συγκεκριμένη λέξη κλειδί. Για παράδειγμα, ονόματα και συνθηματικά χρήστη που χρησιμοποιούνται για μεταφορά αρχείων, για το ηλεκτρονικό ταχυδρομείο και για άλλες υπηρεσίες μπορούν να αναζητηθούν χρησιμοποιώντας λέξεις κλειδιά όπως “USER”, “PASS” και “login” όπως φαίνονται παρακάτω με τη βοήθεια του εργαλείου ngrep σε UNIX.

```
examiner1% ngrep -w 'USER|PASS|login' -t -x -s 65535 -I case02-04032003.dmp
```

```
input: case02-04032003.dmp
match: ((^USER|PASS\W) | (\WUSER|PASS$) | (\WUSER|PASS\W) )
####################################
T 2003/04/03 10:07:39.066816 192.168.0.5:32788      →      172.16.1.10:21 [AP]
   55 53 45 52 20 61 72 67      6f 6e 69 6d 6f 6e 0d        0a    USER argonimon..
##########
T 2003/04/03 10:08:01.956350 192.168.0.5:32788      →      172.16.1.10:21 [AP]
   50 41 53 53 20 70 61 73      73 77 6f 72 64 2d 72        65    PASS password-re
   76 65 61 6c 65 64 0d 0a                                          vealed..
##########
T 2003/04/03 10:24:59.182353 192.168.0.5:32869      →      172.16.1.23:143 [AP]
   32 20 6c 6f 67 69 6e 20      22 6e 61 6d 65 22 20 22      2 login "name" "
   70 61 73 73 77 6f 72 64      2d 72 65 76 65 61 00 00      password-revea..
   09 01 00 00                                                    ...
...##############################################exit
```

Παρόμοια όταν εξετάζουμε για συνδέσεις στο IRC, η αναζήτηση για ψευδώνυμα και ονόματα καναλιών μπορούν να παρέχουν όλη την πληροφορία που χρειάζεται ο ψηφιακός ερευνητής. Για παράδειγμα αναζητώντας το προηγούμενο αρχείο tcpdump για πακέτα που περιλαμβάνουν τη λέξη κλειδί “POST” μπορεί να αποκαλυφθεί η ενέργεια ενός υπόπτου που αποστέλλει ένα μήνυμα.

Όταν διαχειριζόμαστε μεγάλο όγκο δεδομένων που περιλαμβάνουν πολλά τερματικά συστήματα είναι συχνά απαραίτητο να επικεντρωθούμε στη διερεύνηση σε συγκεκριμένα πρωτόκολλα ή σε κίνηση από και προς συγκεκριμένα συστήματα. Το πρόγραμμα tcpdump επιτρέπει το φιλτράρισμα βάσει συγκεκριμένων κριτηρίων αλλά χρησιμοποιεί τη σύνταξη του φίλτρου libpcap που είναι περίπλοκη. Επιπλέον το tcpdump μπορεί να αναγνωρίσει και να εξάγει ένα περιορισμένο αριθμό πρωτοκόλλων συμπεριλαμβανομένων των TCP και UDP. Για να εξαχθεί μόνο η διαδικτυακή κίνηση θα μπορούσε να ελεγχθεί μόνο η κίνηση στην θύρα 80 αλλά αυτή η επιλογή του θα αγνοούσε τη σχετική κίνηση διαδικτύου εάν ο διακομιστής χρησιμοποιούσε διαφορική θύρα όπως την 8080.

Το λογισμικό Argus μπορεί να χρησιμοποιηθεί για να εξετάσει αρχεία του tcpdump και χρησιμοποιεί μία παρόμοια σύνταξη φιλτραρίσματος όπως το tcpdump αλλά έχει πολύ περισσότερες επιλογές και

παρακολουθεί πληροφορίες της κατάστασης συνόδου. Το Ethereal παρέχει μεγαλύτερη λειτουργικότητα φιλτραρίσματος χρησιμοποιώντας μία λίγο πολυπλοκότερη σύνταξη και επίσης υποστηρίζει μεγαλύτερο αριθμό πρωτοκόλλων. Βέβαια αν και το Ethereal υποστηρίζει περισσότερα πρωτόκολλα από το tcpdump, κάνει υποθέσεις σχετικά με την αναμενόμενη συμπεριφορά των πρωτοκόλλων που το αποτρέπουν από την αυτόματη ταξινόμηση της κίνησης η οποία δεν ικανοποιεί αυτές τις βασικές υποθέσεις.

Ορισμένα εμπορικά προγράμματα παρέχουν περισσότερες λειτουργίες από τα δωρεάν αυτά εργαλεία και υλοποιούν φιλτράρισμα και ταξινόμηση της κίνησης. Η γραφική διεπιφάνεια χρήστη του NetIntercept επιτρέπει στον αναλυτή να επιλέξει κριτήρια φιλτραρίσματος όπως οι διευθύνσεις IP πηγής και προορισμού μέσα σε μία συγκεκριμένη χρονική περίοδο. Επίσης το NetIntercept μεταφράζει τα πρωτόκολλα που χρησιμοποιούνται αντί να κάνει υποθέσεις για τις προεπιλεγμένες θύρες που χρησιμοποιεί το καθένα από αυτά. Μεταφράζοντας τα πρωτόκολλα, το εργαλείο αυτό μπορεί να εξάγει αξιοσημείωτο αριθμό συστατικών και να τα αποθηκεύσει σε μία βάση δεδομένων για να υλοποιήσει διερεύνηση και ανάλυση. Η λειτουργία ανάλυσης πρωτοκόλλων είναι επίσης χρήσιμη για να ανακαλυφθεί η κίνηση που παραβιάζει την αναμενόμενη συμπεριφορά, όπως για παράδειγμα ένα διακομιστής FTP ο οποίος εκτελείται σε μία ασυνήθιστη θύρα. Το NetIntercept καταγράφει όλες αυτές τις ανωμαλίες και μπορεί να δημιουργήσει μία αναφορά αυτής της πληροφορίας. Το NetIntercept μπορεί να παράξει αναφορές για την κίνηση δικτύου συμπεριλαμβανομένων και των στατιστικών κίνησης δικτύου.

Συχνά είναι επιθυμητή η αναδημιουργία των σχετικών πακέτων σε πλήρη μηνύματα ή συνόδους. Για παράδειγμα δεδομένα που εμπεριέχονται σε καταγεγραμμένα πλαίσια μπορούν να συνδυαστούν και να δημιουργήσουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μία ιστοσελίδα. Το εργαλείο Ethereal μπορεί να χρησιμοποιηθεί για να αναδημιουργήσει ροές δεδομένων με μία βασική μορφοποίηση αλλά δε μπορεί να διαχειριστεί μεγάλο όγκο δεδομένων.

Ορισμένα εμπορικά εργαλεία είναι ειδικά σχεδιασμένα για ψηφιακή διερεύνηση και παρέχουν πολλές λειτουργίες οπτικοποίησης που κάνουν αποτελεσματικότερη την εξέταση μεγάλου όγκου δικτυακής κίνησης. Για παράδειγμα, το NetIntercept μπορεί να αναδημιουργήσει και να εξάγει περιεχόμενο από την δικτυακή κίνηση, όπως ιστοσελίδες, αρχεία που μεταδόθηκαν μέσω FTP, και αρχεία Word που περιέχονται σε επισυνάψεις μηνυμάτων κωδικοποιημένα με MIME. Επίσης το

NetIntercept για να προστατέψει το υπολογιστικό σύστημα του ερευνητή από κακόβουλο κώδικα, παρουσιάζει τις ιστοσελίδες που αναδημιουργήθηκαν σε ένα προστατευμένο περιβάλλον που δεν εκτελεί κώδικα αλλά τα παρουσιάζει σε πρωτογενή μορφή ώστε να διευκολυνθεί η ανάλυση.

2.6. Διερεύνηση δικτύων στο επίπεδο μεταφοράς

Οι ενέργειες που συμβαίνουν στο επίπεδο δικτύου και στο επίπεδο μεταφοράς παράγουν πληροφορία που είναι συχνά καίρια για την διερεύνηση. Τα αρχεία καταγραφής περιέχουν πληροφορίες σχετικά με τις ενέργειες σε ένα δίκτυο, όταν αυτές συνέβησαν, καθώς και τις διευθύνσεις IP των εμπλεκόμενων μηχανημάτων. Οι πίνακες κατάστασης περιέχουν πληροφορίες, συμπεριλαμβανομένων των διευθύνσεων IP, σχετικά με τις τρέχουσες ή πολύ πρόσφατες συνδέσεις μεταξύ των τερματικών συστημάτων. Οι διευθύνσεις IP στα αρχεία καταγραφής και τους πίνακες κατάστασης μπορούν να χρησιμοποιηθούν για να καθορίσουν την προέλευση της εγκληματικής ενέργειας. Επιπλέον αυτές οι πηγές των ψηφιακών αποδεικτικών στοιχείων είναι χρήσιμες για την διαδικασία αναδημιουργίας και είναι υψίστης σημασίας για την απόδειξη της εγκληματικής πράξης.

Δεδομένης της κεντρικής θέσης που έχει στα δίκτυα το πρωτόκολλο TCP/IP δεν πρέπει να μας προκαλεί έκπληξη ότι οι διευθύνσεις IP, οι αριθμοί θύρας, οι σημαίες TCP, αλλά και άλλα δεδομένα σχετικά με το επίπεδο μεταφοράς TCP/IP συσσωρεύονται σε πολλά σημεία. Η κατανόηση της αναζήτησης και εκμετάλλευσης των πηγών των ψηφιακών αποδεικτικών στοιχείων είναι σημαντική στη διερεύνηση δικτύων. Οι καταγραφές αρχείων των sniffer περιλαμβάνουν πληροφορίες σχετικές με το TCP/IP. Για παράδειγμα ένας εισβολέας χρησιμοποιώντας ένα sniffer σε ένα απομακρυσμένο σύστημα κατέγραφε ονόματα και κωδικούς χρήστη, τα οποία αποθηκευόταν σε ένα αρχείο στον υπολογιστή στόχο. Σε συνδυασμό με το γεγονός αυτό, αποθηκευόταν στο αρχείο οι μη εξουσιοδοτημένες συνδέσεις που έκανε ο εισβολέας στο σύστημα καταγράφοντας και τη δική του διεύθυνση IP. Αν και τα δεδομένα TCP/IP μπορούν να καταγραφούν χρησιμοποιώντας ένα sniffer, η καταγραφή όλης της δικτυακής κίνησης δεν είναι πάντα εφικτή σε όλες τις περιπτώσεις, κάνοντας με τον τρόπο αυτό απαραίτητη την εξάρτηση από άλλες πηγές συλλογής ψηφιακών αποδεικτικών στοιχείων, όπως τα αρχεία καταγραφής που δείχνουν τις προγενέστερες συνδέσεις και πίνακες κατάστασης οι οποίοι δείχνουν τις πρόσφατες και τρέχουσες συνδέσεις μεταξύ των υπολογιστικών συστημάτων.

2.6.1 Αρχεία καταγραφής αυθεντικοποίησης χρήστη

Τα αρχεία αυθεντικοποίησης χρήστη αποτελούν χρήσιμη πηγή ψηφιακών αποδεικτικών στοιχείων καθώς συσχετίζουν τη δραστηριότητα ενός λογαριασμού και συχνά περιλαμβάνουν τη σχετική διεύθυνση IP με τη δραστηριότητα αυτή.

Οι οργανισμοί χρησιμοποιούν κεντρικούς διακομιστές αυθεντικοποίησης ώστε να γίνει η διαχείριση λογαριασμών ευκολότερη σε σχέση με τη χρησιμοποίηση διαφορετικών λογαριασμών χρήστη σε κάθε υποσύστημα. Επομένως οι διαχειριστές δικτύου μπορούν να αναζητήσουν για σχετικά αρχεία καταγραφής αυθεντικοποίησης ώστε να αποκτηθεί ο απαιτούμενος τύπος πληροφορίας και ένας λογαριασμός χρήστη να συσχετιστεί με μία διεύθυνση IP σε μία δεδομένη χρονική στιγμή. Για παράδειγμα ένας διακομιστής αυθεντικοποίησης, είναι ο Microsoft Internet Authentication Server (IAS) και ένας κεντρικός μηχανισμός αυθεντικοποίησης ο οποίος χρησιμοποιείται ευρύτατα είναι ο Kerberos. Αυτά τα συστήματα αυθεντικοποίησης από ένα κεντρικό σημείο μπορούν να αποτελέσουν μία πολύ χρήσιμη και αξιόπιστη πηγή ψηφιακών αποδεικτικών στοιχείων γιατί συσχετίζουν γεγονότα από πολλαπλές πηγές στο δίκτυο, και αποθηκεύουν τα αρχεία καταγραφής σε ένα σύστημα που είναι γενικότερα πιο ασφαλές από τα άλλα συστήματα στο δίκτυο.

Οι διακομιστές ηλεκτρονικού ταχυδρομείου καθώς και άλλοι διαδικτυακοί διακομιστές διατηρούν αρχεία καταγραφής αυθεντικοποίησης χρήστη τα οποία είναι χρήσιμα για τη σύνδεση των διαδικτυακών ενεργειών με ένα πρόσωπο. Ένα παράδειγμα μπορούμε να δώσουμε παρακάτω όπου παρουσιάζεται το αρχείο καταγραφής ενός διακομιστή ηλεκτρονικού ταχυδρομείου όπου χρησιμοποιείται ο λογαριασμός “eco” για να ελεγχθούν τα μηνύματα ηλεκτρονικού ταχυδρομείου από την διεύθυνση IP 10.10.2.10 στις 11:01 και στις 15:02 στις 6 Φεβρουαρίου.

Feb 6 11:01:26 mailsrv ipop3d[26535]: Login user=eco
host =dialup.domain.net [10.10.2.10]
Feb 6 11:01:28 mailsrv ipop3d[26535]: Logout user=eco
host=dialup.domain.net [10.10.2.10]
Feb 6 15:02:48 mailsrv ipop3d[244]: Login user=eco
host=dialup.domain.net [10.10.2.10]
Feb 6 15:02:49 mailsrv ipop3d[244]: Logout user=eco

host=dialup.domain.net [10.10.2.10]

2.6.2 Αρχεία καταγραφής εφαρμογών

Πολλές εφαρμογές δημιουργούν αρχεία καταγραφής εκτός από αυτά των αρχείων καταγραφής αυθεντικοποίησης, και περιλαμβάνουν πληροφορίες σχετικές με τις δραστηριότητες των χρηστών σε ένα δίκτυο και είναι ιδιαίτερα χρήσιμες καθώς περιλαμβάνουν λεπτομέρειες για να αναγνωριστούν τα χαρακτηριστικά της επίθεσης ακόμη και όταν χρησιμοποιούνται λιγότερο συνηθισμένες εφαρμογές.

Για παράδειγμα όταν ένας διαδικτυακός διακομιστής δέχεται ένα αίτημα από μία εφαρμογή πελάτη, καταγράφει την διεύθυνση IP του πελάτη στο αρχείο καταγραφής, μαζί με την ημερομηνία, ώρα και τα αντικείμενα που αιτήθηκε ο πελάτης. Πέρα όμως, από την αποκάλυψη των αιτήσεων από τη διεύθυνση IP που χρησιμοποίησε ο ύποπτος, τα αρχεία καταγραφής της διαδικτυακής προσπέλασης μπορούν να καθορίσουν την διεύθυνση IP που προσπέλασε μία συγκεκριμένη ιστοσελίδα σε μία συγκεκριμένη χρονική στιγμή.

Για να κατανοήσουμε καλύτερα την εξαγώγιμη πληροφορία από τα αρχεία καταγραφής, είναι χρήσιμο να συγκρίνουμε την συνηθισμένη συμπεριφορά των εφαρμογών με μία πιο ασυνήθιστη συμπεριφορά. Όταν ένας χρήστης στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, η ενέργειά του καταγράφεται σε ένα αρχείο καταγραφής στον διακομιστή μηνυμάτων ηλεκτρονικού ταχυδρομείου όπως βλέπουμε παρακάτω:

Feb 7 15:05:30 mailsrv sendmail[1257]: PAA01257: from=(eco@
corpus-delicti.com), size=793, class=0, pri=30793, nrcpts=1,
msgid=(4.2.0.58.19991013150621.0099fa90@mailsrv.corpus-delicti.com),
proto=ESMTP, relay=dialup.domain.net [10.10.2.101]

Feb 7 15:05:31 mailsrv sendmail[1259]: PAA01257: to=bturvey@
corpus-delicti.com, delay=00:00:03, xdelay=00:00:00, mailer=relay,
relay=mail.domain.net. [10.10.2.11], stat=Sent (PAA00253 Message accepted

for delivery)

Να σημειώσουμε ότι ένα μοναδικό μήνυμα δημιουργεί δύο καταχωρήσεις σε ένα αρχείο καταγραφής στον διακομιστή μηνυμάτων ηλεκτρονικού ταχυδρομείου, συμπεριλαμβάνοντας τις λεπτομέρειες του αποστολέα αλλά και του λήπτη, αλλά και οι δύο καταχωρήσεις περιλαμβάνουν το ίδιο αναγνωριστικό μηνύματος. Σε αυτό το υπόδειγμα, η διεύθυνση IP του αποστολέα ήταν η 10.10.2.101. Παρακάτω βλέπουμε τις εγγραφές ενός αρχείου καταγραφής στην περίπτωση που κάποιος παραποιήσει ένα μήνυμα ηλεκτρονικού ταχυδρομείου:

Oct 15 01:20:09 mailserver sendmail[27941]: BAA27941:
from=forged.from@home.net, size=114, class=0, pri=30114, nrcpts=1,
msgid=<199910150518.BAA27941@mailserver>, proto=SMTP,
relay=host1.domain.net [20.134.161.6]

Oct 15 01:20:10 mailserver sendmail[28214]: BAA27941:
to=target@ayyahoo.com, delay=00:01:14, xdelay=00:00:01, mailer=esmtp,
relay=192.168.1.50, stat =Sent (BAA08487 Message accepted for delivery)

Ο πλαστογράφος προφανώς έκανε ένα τυπογραφικό λάθος στην διεύθυνση αποστολής με αποτέλεσμα η κεφαλίδα του μηνύματος ηλεκτρονικού ταχυδρομείου να περιλαμβάνει και άλλους χαρακτήρες, (για παράδειγμα target\bl@ayyahoo.com) όταν δούμε το αποτέλεσμα της ενέργειας σε δεκαεξαδική μορφή.

2.6.3 Αρχεία καταγραφής λειτουργικών συστημάτων

Η πλειονότητα των λειτουργικών συστημάτων μπορούν να διατηρήσουν αξιοσημείωτα γεγονότα όπως επανεκκινήσεις συστήματος, σφάλματα, χρήση του μόντεμ, και κάρτες διεπαφής δικτύου που χρησιμοποιούνται με sniffer. Τα αρχεία καταγραφής στα συστήματα UNIX διατηρούν περισσότερες πληροφορίες σχετικές με το πρωτόκολλο TCP/IP σε σχέση με τα αρχεία καταγραφής γεγονότων των Windows NT, καθώς τα συστήματα UNIX σχεδιάστηκαν αρχικά με γνώμονα τη δικτύωση συστημάτων. Τα περισσότερα αρχεία καταγραφής συστήματος στο UNIX περιλαμβάνουν

πληροφορίες σχετικά με την εισερχόμενη κίνηση, αλλά όχι την εξερχόμενη κίνηση. Το γεγονός αυτό κάνει σχετικά εύκολο τον καθορισμό των ενεργειών ενός ατόμου σε ένα σύστημα αλλά κάνει δύσκολο τον καθορισμό των ενεργειών του ατόμου μακριά από αυτό το σύστημα.

2.6.4 Αρχεία καταγραφής δικτυακών συσκευών

Λόγω του κεντρικού τους ρόλου οι δικτυακές συσκευές συχνά δημιουργούν αρχεία καταγραφής που παρέχουν μία επισκόπηση των ενεργειών σε ένα δίκτυο. Αυτή η γενική προσέγγιση μπορεί να βοηθήσει τους ερευνητές να αποκτήσουν μία βασική κατανόηση των γεγονότων που έγιναν καθώς και των εμπλεκόμενων συστημάτων. Αυτά τα αρχεία καταγραφής παρέχουν λεπτομέρειες των δραστηριοτήτων που δεν καταγράφονται σε άλλα αρχεία. Ακόμη και εάν οι ενέργειες αυτές καταγράφονται από άλλα συστήματα, τα αρχεία καταγραφής των διαδικτυακών συσκευών μπορούν να χρησιμοποιηθούν για επιβεβαίωση, παρέχοντας ανεξάρτητη πηγή ψηφιακών αποδεικτικών στοιχείων που σχετίζονται με τα ίδια συμβάντα.

Ανάλυση περίπτωσης

Ένας οργανισμός ανακάλυψε ότι ένα υπολογιστής στο σύστημα τους έχει παραβιαστεί χρησιμοποιώντας μία ευπάθεια που δεν είχε ανιχνευθεί από το σύστημα ανίχνευσης παρείσφρησης. Τα αρχεία καταγραφής του NetFlow εξετάστηκαν για να κατανοήσουμε πλήρως τον τρόπο που παραβιάστηκε το υπολογιστικό σύστημα. Τα αρχεία καταγραφής του NetFlow έδειξαν ότι περίπου στις 12:25 πμ. της 21 Οκτωβρίου, η διεύθυνση adsl-61-105-217.msy.bellsouth.net (208.61.105.217) είχε ως στόχο την διεργασία SSH daemon στο παραβιασμένο σύστημα. Η ενέργεια που αναγνωρίστηκε συνοδευόταν από τα ακόλουθα αρχεία καταγραφής συστήματος:

```
Oct 21 00:29:25 hostA sshd[18967]: connect from 208.61.105.217
Oct 21 00:29:25 hostA sshd[18967]: log: Connection from 208.61.105.217
port 4584
Oct 21 00:29:34 hostA sshd[18967]: fatal: Did not receive ident string.
```

Περίπου στις 02:15 πμ. της 21 Οκτωβρίου, τα αρχεία καταγραφής του NetFlow έδειξαν ότι η

διεύθυνση IP 66.28.12.53 προσπέλασε τον διακομιστή SSH. Το γεγονός αυτό συνοδεύταν από υπερχείλιση του buffer που καταγράφηκε στο αρχείο syslog του παραβιασμένου υπολογιστικού συστήματος:

```
Oct 21 02:16:24 hostA sshd[18997]: connect from 66.28.12.53
Oct 21 02:16:24 hostA sshd[18997]: log: Connection from 66.28.12.53 port 2974
Oct 21 02:16:24 hostA sshd[18997]: log: Could not reverse map address
66.28.12.53.
Oct 21 02:16:25 hostA sshd[18998]: connect from 66.28.12.53
Oct 21 02:16:25 hostA sshd[18998]: log: Connection from 66.28.12.53 port 2975
Oct 21 02:16:25 hostA sshd[18998]: log: Could not reverse map address
66.28.12.53.
<cut or brevity>
Oct 21 02:18:29 hostA sshd[19119]: fatal; Local: crc32 compensation attack:
network attack detected
```

Σε αυτό το σημείο ο εισβολέας εγκατέστησε ένα IRC bot και ένα ident daemon για να αποκρίνεται στους διακομιστές IRC με άλλο όνομα πέρα από αυτό του χρήστη root. Αρκετοί διακομιστές IRC δεν αποδέχονται συνδέσεις από τον λογαριασμό χρήστη root ενός συστήματος διότι το αναγνωρίζουν σαν ένα δείγμα παραβίασης του συστήματος:

```
Oct 21 02:46:37 hostA in.ident2[28529]: error: setuid(-2): Paramère invalide
Oct 21 02:46:37 hostA in.ident2[28529]: error; cannot reduce self's rights
```

Επίσης ο εισβολέας αντικατέστησε το SSH με μία έκδοση του που περιελάμβανε δούρειο ίππο και κατέγραφε το συνθηματικά χρήστη σε ένα αρχεία με όνομα "/usr/lib/libfl.so.3.". Αυτή η τροποποιημένη διεργασία είχε επίσης ένα κενό ασφαλείας τύπου που σχετιζόταν με το όνομα χρήστη "smiley":

```
# strings sshd
Rhosts with RSA authentication disabled.
RSA_new failed
```

BN_new failed

Warning: keysize mismatch for client_host_key: actual %d, announced %d

RSA authentication disabled.

Password authentication disabled.

smiley

/usr/lib/libfl.so.3

user: %s

password: %s

rcvd SSH_CMSG_AUTH_TIS

Επιπλέον, ο εισβολέας αντικατέστησε το αρχείο "/bin/login" με μία μολυσμένη έκδοση που λειτουργεί ως δούρειος ίππος, η οποία επέτρεπε την πρόσβαση σε ένα σύστημα εάν η μεταβλητή DISPLAY του πελάτη έχει τεθεί σε “smiley”. Ανιχνεύοντας το δίκτυο για άλλα συστήματα με τα ίδια κενά ασφαλείας αποκάλυψε δύο ακόμη παραβιασμένα συστήματα. Ο εισβολέας επιτέθηκε στα συστήματα αυτά από διαφορετική διεύθυνση IP. Αυτός είναι και ο λόγος που δεν εμφανίστηκαν στην αρχική διερεύνηση των αρχείων καταγραφής του Netflow. Βέβαια ίδια την χρονική στιγμή που έγινε αντιληπτή η διάσταση της εισβολής στο σύστημα, τα αρχεία καταγραφής του NetFlow τα οποία είχαν δημιουργεί αρχικά, αντικαταστάθηκαν με αποτέλεσμα να μην είναι δυνατός ο εντοπισμός των ενεργειών του εισβολέα στα άλλα συστήματα. Τέλος τα αρχεία καταγραφής του IRC bot ήταν κρυπτογραφημένα αποτρέποντας τους ερευνητές από την απόκτηση επιπλέον πληροφοριών σχετικά με τον εισβολέα. (Casey et al,2004)

2.6.5 Πίνακες κατάστασης

Οι πίνακες κατάστασης περιλαμβάνουν πληροφορίες σχετικά με την παρούσα και πολύ πρόσφατη κατάσταση των συνδέσεων μεταξύ των υπολογιστών. Τα δεδομένα στους πίνακες κατάστασης είναι προσωρινά, δηλαδή οι ανενεργές καταχωρήσεις συνήθως διαγράφονται μέσα σε μία ώρα. Οι πίνακες κατάστασης διατηρούν τις ενεργές και πρόσφατες συνδέσεις από συσκευές όπως τείχη προστασίας, δρομολογητές και άλλες δικτυακές συσκευές. Αυτές οι πληροφορίες χρησιμοποιούνται για να ενισχύσουν άλλα αποδεικτικά στοιχεία και να αποδειχθεί η συνέχεια του εγκλήματος.

Ένα παράδειγμα των πινάκων κατάστασης είναι οι πρόσφατες συνδέσεις NetBIOS οι οποίες διατηρούνται από τα Windows ως μία λίστα ονομάτων NetBIOS και οι διευθύνσεις IP στον πίνακα ονομάτων NetBIOS. Το παρακάτω παράδειγμα περιλαμβάνει την εφαρμογή VNC, τον πίνακα ονομάτων του μηχανήματος Windows XP στο οποίο εκτελείται ο διακομιστής VNC, με IP 192.168.0.4, και είχε μία σύνδεση NetBIOS με IP 192.168.0.2.

```
C:\> nbtstat -c

                NetBIOS Remote Cache Name Table

    Name                Type        Host Address        Life [sec]
    ---------------------------------------------------------------
    WORKSTN2            <20> UNIQUE     192.168.0.2         567
```

Οι εισερχόμενες συνδέσεις NetBIOS μπορούν να επισκοπηθούν χρησιμοποιώντας την εντολή net session αλλά δεν εμφανίζεται η συσχετιζόμενη διεύθυνση IP. Για παράδειγμα εκτελώντας την εντολή του προηγούμενου παραδείγματος μπορούμε να δούμε ποιος λογαριασμός χρήστη χρησιμοποιήθηκε για την εγκαθίδρυση της σύνδεσης στη σύνοδο NetBIOS, παρέχοντας μόνο το όνομα NetBIOS του μηχανήματος Windows XP.

```
C:\>net session

    Computer        User name       Client Type         Opens Idle time
    ---------------------------------------------------------------------
    \\WORKSTN1      USER1           Windows 2002 2600   0 00:00:23

    The command completed successfully.
```

Όμοια με παραπάνω, τα συστήματα UNIX διατηρούν μία λίστα των απομακρυσμένων μηχανημάτων που έχουν συνδεθεί στο διαμοιραζόμενο σύστημα αρχείων. Παρακάτω βλέπουμε το αποτέλεσμα χρησιμοποιώντας την εντολή showmount:

[nfs-server]# showmount -a .

All mount points on case:

192.168.0.101;/Shared-drive

Στο τερματικό του πελάτη, η εντολή mount εμφανίζει όλα τα διαμεριζόμενα αρχεία τα οποία προσπελάστηκαν απομακρυσμένα.

[nfs-client]# [mount

<entries relating to local drives cut for brevity>

/mnt on 192.168.0.7:/ remote/read/write/nosetuid/dev=2f80002 on Thu Apr

10 08:31:19 2003

Αυτές οι εντολές χρησιμοποιούνται στις διερευνήσεις δικτύων ώστε να καθοριστούν τα συστήματα τα οποία συνδέθηκαν με το δεδομένο σύστημα. (Casey et al,2004)

2.6.6 Περιεχόμενα μνήμης RAM

Δεδομένα σχετικά με το TCP/IP περιλαμβάνονται στη μνήμη RAM κάθε τερματικού συστήματος, συμπεριλαμβανόμενων των διακομιστών, των δρομολογητών και των τειχών προστασίας. Εξάγοντας τα περιεχόμενα της μνήμης RAM είναι πιθανό να ανακτήσουμε τις διευθύνσεις IP και άλλα χρήσιμα δεδομένα σχετικά με τη δραστηριότητα δικτύου. Για παράδειγμα, ένας εισβολέας ενός υπολογιστικού συστήματος χρησιμοποιεί ένα κλεμμένο λογαριασμό για να εγκαταστήσει ένα IRC bot, το οποίο επιτρέπει σε διάφορους χρήστες να συνδεθούν στο IRC μέσω ενός παραβιασμένου τερματικού, ώστε να αποκαλυφθεί η πραγματική IP τους σε άλλα άτομα στο IRC. Η κίνηση αν και είναι κρυπτογραφημένη μεταξύ των δύο τερματικών συστημάτων και του IRC bot, είναι δυνατό να αποκτήσουμε κάποιες πληροφορίες εξετάζοντας τα περιεχόμενα της μνήμης:

% **/mnt/cdrom/static-binaries/solaris/last stolenaccount**

stolenaccount pts/18 Apr 18 12:34 mail.almustaqbal.com.lb - 12:58 (00:24)

% **/mnt/cdrom/static-binaries/solaris/ps -ef | grep stolenaccount**

root 3485 2432 0 18:05:03 pts/17 0:00 grep stolenaccount

root 3430 2387 0 18:04:37 pts/10 0:00 script stolenaccount.04182003
stolenaccount 9455 1 0 Apr 17 ? 0:01 ./tcsh unf
stolenaccount 13961 1 0 Apr 17 ? 0:01 ./bnc

% /mnt/cdrom/static-binaries/solaris/gcore -o /mnt/evidence/core 9455
gcore: /mnt/evidence/core.9455 dumped
% /mnt/cdrom/static-binaries/solaris/gcore -o /mnt/evidence/core 13961
gcore:/mnt/evidence/core.13961 dumped
% cd /mnt/evidence
% strings - core.9455 | more
<cut for brevity>
PART #cavite
a QUIT :sTiLL dA oNe i wAnT...sTiLL dA oNe i LoVeCAVITE's WebSite
(www.cavitechannel.com)
8.244 PRIVMSG #cavite:
0, 0**********
4, 4***
8, 8***
1, 12********* GoodByE all *********
8, 8***
4, 4***
:CuCuMbEr-!v2000@**210.23.248.244** PRIVMSG #cavite :
<cut for brevity>

DjCuRe **210.23.248.165** graz.at.Eu.UnderNet.org djcure H :4G
:McLean.VA.us.undernet.org 352 boseman #cavite SMuRF **210**.**23**.**248.163**
Amsterdam.NL

.Eu.UnderNet.org explorer2H :4
2, 15
:McLean.VA.us.undernet.org 352 boseman #cavite ofm_cap **nova4117.**
i-next.net Manha

ttan.KS.US.Undernet.Org Jhayr H :3 FERNANDO JOSE

:McLean.VA.us.undernet.org 352 boseman #cavite ~clarice **web.cyworld.net**

:Arlingto

n.VA.US.Undernet.Org Clarimace H :3 Pls join #Li

Ipid.bnc

fuckj00

<cut for brevity>

Οι δικτυακές συσκευές μπορεί επίσης να περιλαμβάνουν στη RAM κάποιες σχετικές πληροφορίες με το TCP/IP οι οποίες δεν είναι διαθέσιμες από την γραμμή εντολών. Τέλος είναι δυνατό να εξάγουμε τα περιεχόμενα της RAM με σύνδεση μίας ειδικής συσκευής στο σύστημα όπου θα γίνει η διερεύνηση, η οποία έχει τα μειονεκτήματα ότι είναι ακριβή και δυσεφάρμοστη σε δικτυακές συσκευές.

3. Τεχνικές συστηματικής διερεύνησης δικτύων υπολογιστών

Όταν ανιχνευθεί παρείσφρηση σε ένα δίκτυο θα πρέπει να παρθούν κάποια μέτρα με πρώτο βήμα την αναγνώριση και συλλογή των ευαίσθητων δεδομένων. Στην συνέχεια, αναλύονται τα αρχεία καταγραφής με τη χρήση ειδικών εργαλείων τα οποία μπορούν να αποκαλύψουν πληροφορίες σχετικά με την παρείσφρηση όπως το σημείο από όπου ξεκίνησε, εξετάζεται η ευπάθεια του συστήματος που εκμεταλλεύτηκαν οι επιτιθέμενοι και ούτω καθεξής.

3.1 Παρακολούθηση δικτύου και καταγραφή

Η διατήρηση αρχείου καταγραφής, ως μέτρο πρόληψης, παρέχει πολύ χρήσιμες πληροφορίες. Η παρακολούθηση του δικτύου για ύποπτες συνδέσεις ή νέες διεργασίες σε πραγματικό χρόνο, είναι ένας αποτελεσματικός τρόπος για να αναγνωριστούν και να σταματήσουν οι επιθέσεις. Οι προειδοποιήσεις παρείσφρησης ή τα συστήματα ανίχνευσης παρείσφρησης (IDS) ενεργοποιούν την ανάλυση των δικτυακών δεδομένων αλλά δεν παρέχουν καμία πληροφορία σχετικά με τα γεγονότα

που συνέβησαν μετά την επίθεση. Ακόμη μπορεί να αποδειχθεί χρήσιμη η παρακολούθηση των διαδικτυακών συζητήσεων και άλλων μορφών δικτυωμένης επικοινωνίας. Ο ολοένα αυξανόμενος αριθμός δικτυωμένων υπολογιστών και το διογκούμενο διαδίκτυο, δυσκολεύει την παρακολούθηση της κίνησης στο δίκτυο. Επίσης δεν είναι επαρκώς καθορισμένη η χρονική διάρκεια που θα πρέπει διατηρούνται τα αρχεία καταγραφής σε διάφορα σημεία στο δίκτυο. Αυτό εξαρτάται άμεσα από το διαθέσιμο αποθηκευτικό χώρο. Βέβαια η απόκτηση των αρχείων καταγραφής δικτύου είναι δύσκολη μιας και υπόκεινται σε διαφορετικές πολιτικές χρήσης.

3.2 Ιχνηλάτιση ηλεκτρονικού ταχυδρομείου

Τα μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται συνήθως κατά την διάπραξη εγκλημάτων. Εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου σχετίζεται με ένα έγκλημα, θα πρέπει να καταγραφεί ως αποδεικτικό στοιχείο και η κεφαλίδα του μηνύματος ηλεκτρονικού ταχυδρομείου μπορεί να αποδειχθεί χρήσιμη για την ανίχνευση του υπόπτου. Η διαδικασία ιχνηλάτισης ηλεκτρονικού ταχυδρομείου απαιτεί από τον αναλυτή να γνωρίζει καλά τη λειτουργία του ηλεκτρονικού ταχυδρομείου. Κάποια τμήματα της κεφαλίδας ενός μηνύματος ηλεκτρονικού ταχυδρομείου δεν μπορούν να πλαστογραφηθούν τόσο εύκολα, όπως για παράδειγμα ο τελευταίος διακομιστής από όπου προωθήθηκε το μήνυμα ηλεκτρονικού ταχυδρομείου. Τα αρχεία καταγραφής που διατηρούν ο δρομολογητής και το τείχος προστασίας μπορούν να βοηθήσουν στην επιβεβαίωση της διαδρομής του μηνύματος ηλεκτρονικού ταχυδρομείου. Οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου συνήθως διατηρούν ένα αρχείο καταγραφής όλων των ηλεκτρονικών μηνυμάτων που επεξεργάστηκαν. Επομένως ακόμη και εάν ο χρήστης διαγράψει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, αυτό μπορεί να ανακτηθεί από τους διακομιστές ηλεκτρονικού ταχυδρομείου. Βέβαια ανακύπτουν θέματα νομιμότητας και δικαιοδοσίας τα οποία αποτελούν τροχοπέδη για την ιχνηλάτιση μηνυμάτων ηλεκτρονικού ταχυδρομείου. Να σημειώσουμε ότι τα αρχεία καταγραφής δεν διατηρούνται επαρκώς από τους παρόχους υπηρεσιών διαδικτύου (ISPs). Η διαδικασία της ιχνηλάτισης μηνυμάτων ηλεκτρονικού ταχυδρομείου γίνεται ακόμη πιο δύσκολη με κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου και αλλαγές στο πεδίο κεφαλίδας τους.

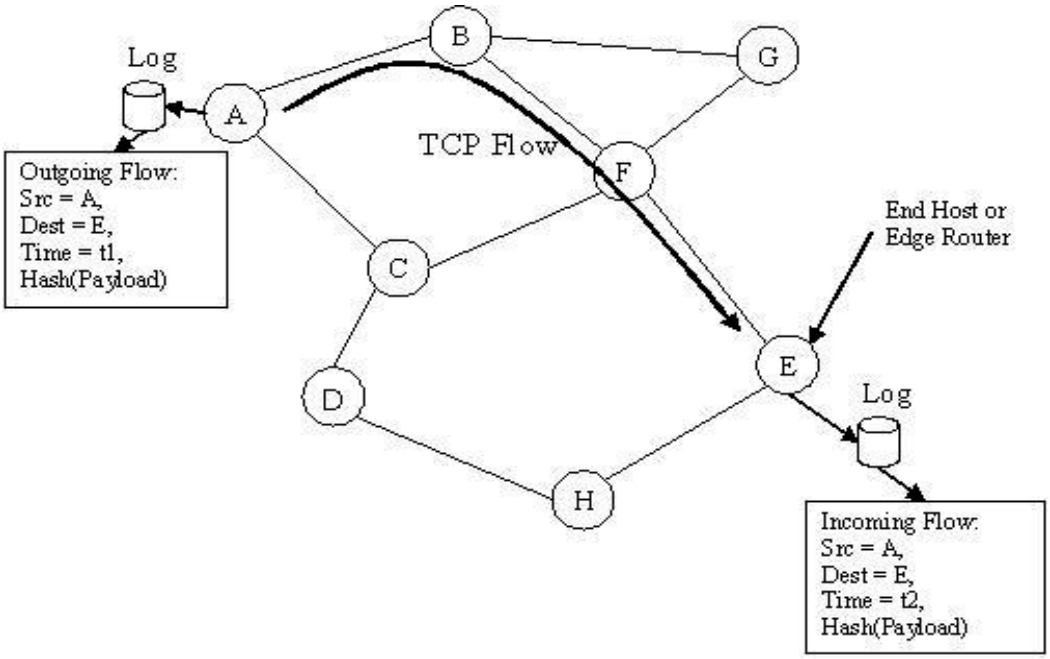
3.3 Αναζήτηση των ιχνών της IP προέλευσης

Οι περισσότερες επιθέσεις άρνησης εξυπηρέτησης (DoS) περιλαμβάνουν ένα μεγάλο αριθμό πακέτων που στέλνονται στον υπολογιστή στόχο. Όλα αυτά τα σχετικά πακέτα έχουν προφανώς έγκυρες διευθύνσεις IP προέλευσης. Βέβαια τα πακέτα δεν παρέχουν καμία πληροφορία που θα βοηθούσε να καθοριστεί το σύστημα του επιτιθέμενου. Η μεθοδολογία IP Traceback αναλαμβάνει τον καθορισμό της προέλευσης αυτών των πακέτων. Ορισμένες τεχνικές IP traceback περιλαμβάνουν εκτέλεση ερωτημάτων προς τους δρομολογητές σχετικά με την κίνηση δικτύου που προωθούν, την δημιουργία εικονικών δικτύων επικάλυψης χρησιμοποιώντας μηχανισμούς καταγραφής για επιλεγμένες ροές πακέτων, και προσδιορισμό της ανασχηματισμένης διαδρομής που ακολούθησε ο επιτιθέμενος, χρησιμοποιώντας μία συλλογή πακέτων, τα οποία είναι είτε επισημασμένα ή ειδικά σχεδιασμένα από τους δρομολογητές κατά μήκος της διαδρομής που ακολουθήθηκε. Να σημειώσουμε ότι δεν υπάρχει σίγουρη λύση ότι θα αναγνωριστεί επιτυχώς η πηγή των επιθέσεων.

3.4 Αναδημιουργία της επίθεσης και των αποδεικτικών στοιχείων

Οι επιθέσεις μέσω διαδικτύου όπως για παράδειγμα τα σκουλήκια και οι ιοί εξελίσσονται όλο και περισσότερο και εξαπλώνονται πολύ γρήγορα χωρίς παρέμβαση του χρήστη. Τα σκουλήκια δεν χρειάζονται παρέμβαση του χρήστη για μεταδοθούν, μιας και είναι κομμάτια κώδικα που πολλαπλασιάζονται από μόνα τους. Η ανίχνευση της πραγματικής πηγής του κακόβουλου λογισμικού αποτελεί γεγονός υψηλής σημαντικότητας της επιστήμης της δικανικής δικτύων. Στην παρακάτω εικόνα βλέπουμε τη διαδρομή επικοινωνίας μεταξύ δύο κόμβων σε ένα δίκτυο. Οι λεπτομέρειες της ροής δεδομένων διατηρούνται τόσο από τον κόμβο πηγή Α, όσο και από τον κόμβο προορισμό Ε, που βρίσκονται κατά μήκος της ροής δεδομένων. Επομένως εάν ανιχνευθεί μία ροή κακόβουλων δεδομένων στον κόμβο Ε, τότε αυτός ο κόμβος αναζητά τον πίνακα διευθύνσεων για εισερχόμενα δεδομένα ώστε να καθορίσει την πηγή των κακόβουλων δεδομένων. Στην συνέχεια ο κόμβος Ε χρησιμοποιεί το πρωτόκολλο ερωτήματος – απόκρισης ώστε να καθορίσει την προέλευση των κακόβουλων δεδομένων. Οι λεπτομέρειες των ροών δεδομένων μπορούν εναλλακτικά να αποθηκευτούν στα άκρα του δικτύου παρά σε τερματικά συστήματα ούτως ώστε να αποφευχθούν τροποποιήσεις στα τερματικά συστήματα.

Η αναδημιουργία της επίθεσης επιτρέπει στους διαχειριστές συστημάτων να κατανοήσουν τους μηχανισμούς διάδοσης των κακόβουλων δεδομένων ούτως ώστε να επιδιορθώσουν τα ευπαθή συστήματα και να αποτρέψουν μελλοντικές επιθέσεις. Η ιχνηλάτιση της προέλευσης μίας διαδικτυακής επίθεσης είναι χρήσιμη για την άσκηση ποινικής δίωξης ή τον μετριασμό του σκοπού της επίθεσης. (Kanellis, 2006)



Εικόνα 6: Ιχνηλάτιση της προέλευσης ενός σκουληκιού μέσω διαδικτύου (Kanellis, 2006)

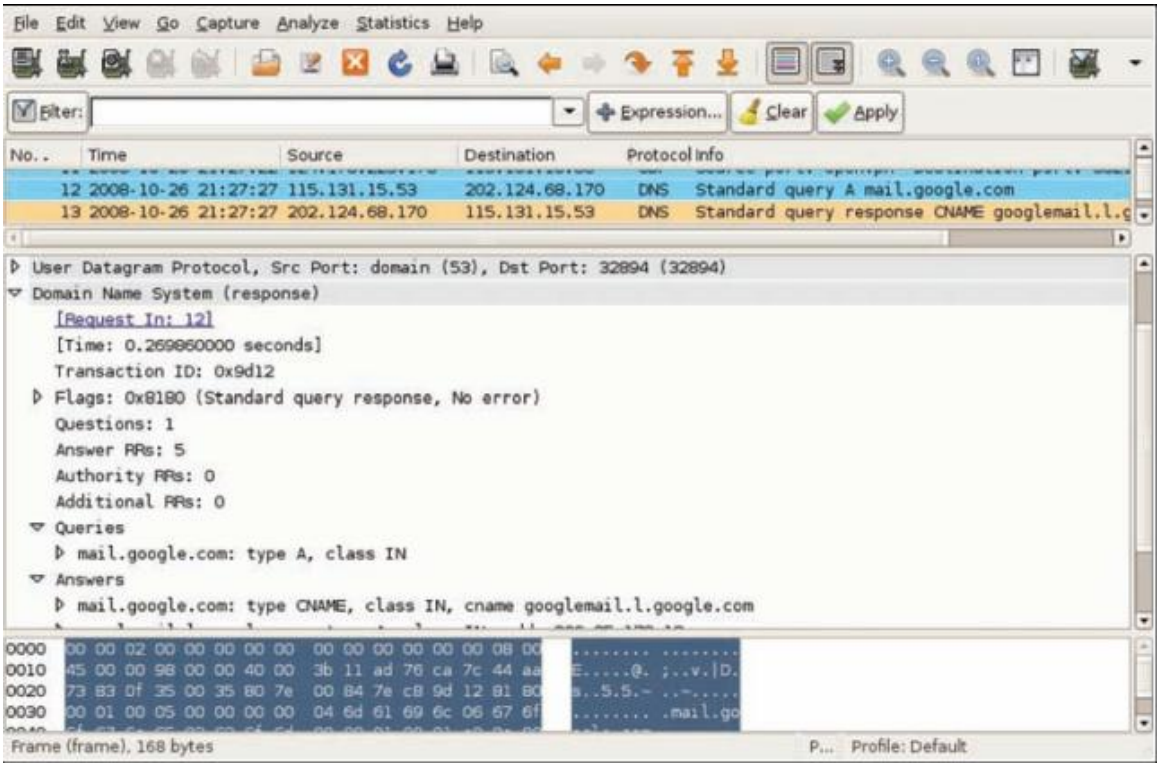
3.5 Διχοτόμηση πακέτων

Όπως γνωρίζουμε τα πρωτόκολλα δικτύων έχουν σχεδιαστεί ως επίπεδα, όπου τα υψηλότερα επίπεδα των πρωτοκόλλων ενσωματώνονται στα χαμηλότερα. Η διαδικασία της αποκωδικοποίησης ενός δικτυακού πακέτου ορίζεται ως διχοτόμηση. Η διχοτόμηση απαιτεί πολύ καλή κατανόηση των δικτυακών πρωτοκόλλων.

Παράδειγμα χρήσης του Wireshark για διχοτόμηση πακέτων

Το Wireshark υλοποιεί διχοτόμηση πακέτων με πολλά εργαλεία, καθώς αυτά τα εργαλεία έχουν

σχεδιαστεί ειδικά για την ανίχνευση διαφορετικών πρωτοκόλλων. Ένα παράδειγμα ενός σημαντικού πακέτου πρωτοκόλλου στην διερεύνηση δικτύων, είναι η υπηρεσία ονομάτων τομέα (DNS), η οποία μας πληροφορεί για την ανάλυση των ονομάτων DNS καθώς τα ονόματα λαμβάνονται από τα δικτυακά δεδομένα. Ο γεγονός αυτό είναι σημαντικό καθώς οι εγγραφές DNS μπορεί να έχουν αλλάξει κατά το χρόνο όπου γίνεται η καταγραφή των δεδομένων σε σχέση με το χρόνο κατά τον οποίο γίνεται η ανάλυση. Όταν έχουμε μία αίτηση DNS για μία εγγραφή A, η απόκριση που θα λάβουμε, θα επιστρέψει μία διεύθυνση IP, και στη συνέχεια μία σύνδεση TCP με αυτήν την διεύθυνση IP. Καταγράφοντας την αναζήτηση DNS είμαστε ικανοί να καθορίσουμε με ποιο τερματικό σύστημα προσπαθεί να επικοινωνήσει το σύστημα μας κατά τη χρονική στιγμή της καταγραφής.



Εικόνα 7: Διχοτόμηση ενός πακέτου DNS με το Wireshark (Li,2010)

3.6 Αναδημιουργία ροής TCP

Συνηθέστερα ενδιαφερόμαστε για την ανάλυση των δεδομένων που μεταδίδονται σε ροές TCP. Η διαδικασία της αναδημιουργίας ξεχωριστών πακέτων που περιέχονται σε μία ροή, σε δεδομένα μέσα

σε μία ροή, καλείτε αναδημιουργία ροής TCP. Η αναδημιουργία ροής TCP είναι ένα χρήσιμο συστατικό κάθε συστήματος για το οποίο χρειάζεται να εξεταστούν οι ροές TCP. Οι πιο συνηθισμένες συσκευές για τις οποίες αποτελεί συστατικό κρίσιμης σημασίας είναι τα συστήματα ανίχνευσης παρείσφρησης δικτύου (NIDS).

Το πρόβλημα της αναδημιουργίας είναι δύσκολο να λυθεί, διότι υπάρχουν πολλές ακολουθίες πακέτων TCP/IP χωρίς προκαθορισμένη ερμηνεία. Για να αναδημιουργήσουμε σωστά τα πακέτα TCP, θα πρέπει να έχουμε καλή γνώση του λειτουργικού συστήματος που εκτελείται στο τερματικό σύστημα καθώς και τη διαμόρφωση του συστήματος. Χωρίς αυτήν την γνώση μπορεί να οδηγηθούμε σε λάθος αναδημιουργία πακέτων TCP τα οποία θα είναι διαφορετικά από τα πραγματικά πακέτα που λήφθηκαν από το τερματικά συστήματα.

Η αναδημιουργία TCP είναι ένας συμβιβασμός ανάμεσα σε πολλές ανταγωνιζόμενες απαιτήσεις. Μία υπόθεση που μπορεί να γίνει είναι ότι η κίνηση δικτύου μπορεί να βρεθεί σε φυσική μορφή. Σύμφωνα με αυτήν τη θεώρηση τα επικοινωνούντα μέρη δεν είναι ενήμερα για την καταγραφή δικτύου που διενεργείται, οπότε δε θα προσπαθήσουν εσκεμμένα να ανατρέψουν την αναδημιουργία TCP διακόπτοντας τις ροές δεδομένων, ώστε οι ροές δεδομένων να καταστούν ασαφείς. Αυτή η υπόθεση μπορεί να μη ισχύει σε κάποιες περιπτώσεις, οπότε ο αναλυτής δικτύου θα πρέπει να εξετάσει εάν η αναδημιουργία της ροής έχει ανατραπεί.

Πέρα από την παραπάνω περίπτωση υπάρχει και η συνδυασμένη ροή, η οποία σχηματίζεται συνδυάζοντας με μία ροή με χρονολογική σειρά, τόσο προς τα εμπρός όσο προς τα πίσω. Συχνά είναι ευκολότερο να αναλύσουμε της συνδυασμένες ροές, ειδικότερα για αμφίδρομα πρωτόκολλα, στέλνοντας μηνύματα απόκρισης - απάντησης. Στην περίπτωση αυτή θα πρέπει να ληφθούν όλα τα δεδομένα του ενός επικοινωνούντος μέρους πριν ξεκινήσει η μετάδοση από το άλλο μέρος.

3.7 Ερμηνεία του πρωτοκόλλου HTTP

Οι ερευνητές δικτύων ενδιαφέρονται περισσότερο για την απόκτηση πληροφοριών υψηλού επιπέδου από την κίνηση του δικτύου, σε σχέση με τις πληροφορίες πρωτοκόλλων χαμηλών επιπέδων. Όταν ένας χρήστης πλοηγείται σε μία ιστοσελίδα, ο περιηγητής ιστού μπορεί να δημιουργήσει πολλές

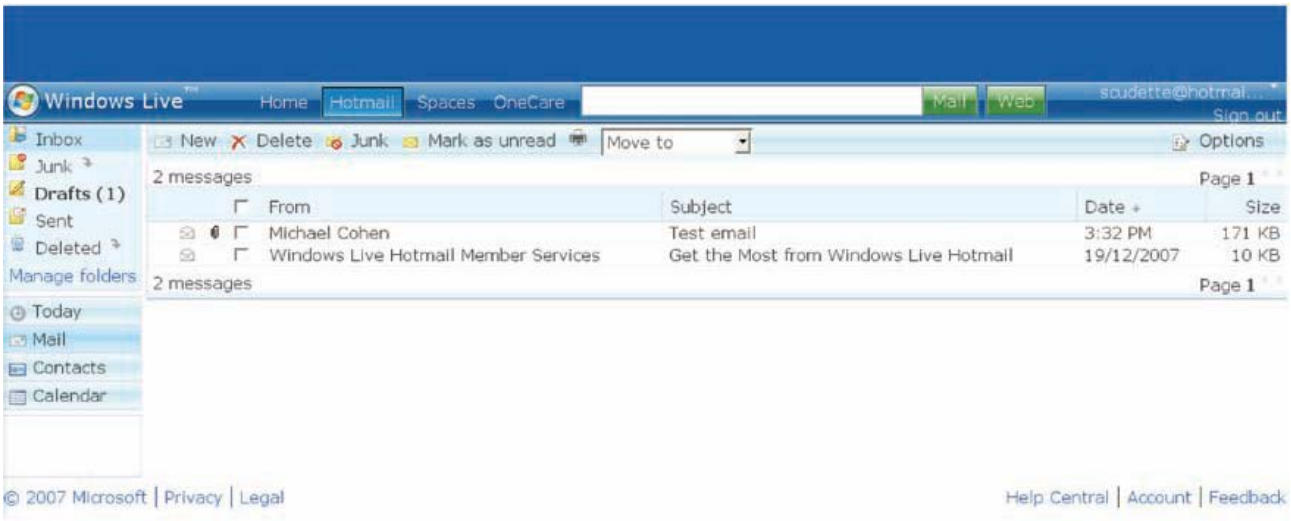
διαφορετικές συνδέσεις HTTP, και να κατεβάσει πολλά διαφορετικά αντικείμενα, όπου όλα θα αναφέρονται στην ίδια ιστοσελίδα.

Ο ερευνητής ενδιαφέρεται να δει την ιστοσελίδα όσο πιο κοντά γίνεται σε σχέση αυτήν με αυτή που είδε ο ύποπτος. Ο όρος Page Rendering αναφέρεται στην αναπαράσταση της σελίδας, όπως αυτή αντλήθηκε από την κίνηση δικτύου, η οποία αποδίδεται όσο πιο πιστά γίνεται σε σχέση με την ιστοσελίδα που είδε ο ύποπτος κατά το χρονικό διάστημα που έγινε η καταγραφή.

Διεύθυνση ιστού	Παράμετροι	Ερμηνεία
google.com	q	Όρος αναζήτησης
gmail.com	subject, to, from	Παράμετροι ηλεκτρονικού ταχυδρομείου

Πίνακας 2: Οι συνηθέστερες παράμετροι οι οποίες είναι σημαντικές από την οπτική γωνία της διερεύνησης δικτύων. (Li, 2010)

Ορισμένες εφαρμογές διερεύνησης δικτύων εξάγουν απλά τον κώδικα HTML και στη συνέχεια αφαιρούν τις αναφορές προς εικόνες και τον κώδικα javascript. Άλλες εφαρμογές διερεύνησης δικτύων, όπως το PyFlag, χρησιμοποιούν ένα περιηγητή ιστού για να αποδώσουν την ιστοσελίδα μεταβάλλοντας τον HTML κώδικα της σελίδας ώστε οι εικόνες και η μορφοποίηση της ιστοσελίδας να αναλυθούν κατά την καταγραφή του δικτύου. Η δεύτερη προσέγγιση μας παρέχει ακριβέστερη οπτική αναπαράσταση της ανακατασκευασμένης ιστοσελίδας. Το ζητούμενο σε αυτή την περίπτωση είναι ότι θέλουμε αυτές οι εικόνες να ανακτηθούν από την καταγραφή δεδομένων της κίνησης δικτύου, δεδομένου ότι δε θέλουμε ο περιηγητής ιστού να κατεβάσει τις εικόνες από τους αυθεντικούς διακομιστές, διότι οι αιτήσεις αυτές μπορεί να εγείρουν υποψίες στον διαχειριστή του διακομιστή. Το αποτέλεσμα από τις ενέργειες αυτές εξαρτάται από την πολυπλοκότητα της ιστοσελίδας και τον κώδικα javascript. Στη περίπτωση όπου η ιστοσελίδα είναι απλή, μπορεί να αποδοθεί με μεγάλη ακρίβεια. Ένα παράδειγμα βλέπουμε παρακάτω:



Εικόνα 8: Η απόδοση μίας ιστοσελίδας όπως την επισκεφτήκαμε από το Hotmail. Όλα τα στοιχεία της ιστοσελίδας συμπεριλαμβανομένης της μορφοποίησής της και των εικόνων ανακτήθηκαν αυτόματα από την καταγραφή δικτύου. (Li, 2010)

3.8 Κρυφή μνήμη του περιηγητή ιστού

Ορισμένες φορές ο περιηγητής ιστού του υπόπτου, μπορεί να περιέχει ορισμένα αρχεία που χρειάζονται για να αποδοθεί σωστά η ιστοσελίδα. Αυτά αρχεία μπορούν να ανακτηθούν από την κρυφή μνήμη του περιηγητή ιστού οπότε ο ύποπτος δε θα αιτηθεί για αυτά τα αρχεία από τον διακομιστή δικτύου. Η κρυφή μνήμη του περιηγητή ιστού μπορεί να διατηρεί αντικείμενα για μεγάλο χρονικό διάστημα, κατά το οποίο ο περιηγητής ιστού δε θα αιτείται για αυτά τα αντικείμενα από διακομιστές δικτύου, αλλά θα κάνει χρήση της κρυφής μνήμης ούτος ώστε να αποδώσει σωστά την ιστοσελίδα. Όπως καταλαβαίνουμε το γεγονός αυτό εγείρει προβλήματα στους ερευνητές δικτύων, καθώς ορισμένες από τις εικόνες αλλά και τα στυλ μορφοποίησης τα οποία είναι απαραίτητα για τη σωστή απόδοση της ιστοσελίδας, βρίσκονται στην κρυφή μνήμη του περιηγητή ιστού, οπότε αυτά τα στοιχεία δε θα μεταδοθούν στο δίκτυο.

Με τη χρήση κάποιων πακέτων λογισμικού δικανικής δικτύων, όπως το PyFlag, υπάρχει η δυνατότητα στους χρήστες να κατεβάσουν κάποια επιλεγμένα αντικείμενα από τις ιστοσελίδες από τις οποίες προέρχονται. Βέβαια ο ερευνητής θα πρέπει να λάβει υπόψη ότι πιθανόν να εγείρει υποψίες στον διαχειριστή του διακομιστή εάν τελικά κατεβάσει τα απαιτούμενα αντικείμενα.

3.9 Εφαρμογές Διαδικτύου – Διαδικτυακό ταχυδρομείο

Τα τελευταία χρόνια υπάρχει η μεγάλη ανάπτυξη εφαρμογών διαδικτύου οι οποίες είναι υλοποιημένες σε γλώσσες προγραμματισμού όπως η AJAX, με αποτέλεσμα να δημιουργούνται αλληλεπιδραστικές εφαρμογές, η σωστή απόδοση των οποίων αποτελεί πρόβλημα για τους ερευνητές της δικανικής δικτύων. Μερικές από αυτές τις εφαρμογές είναι το Gmail, το Google Maps, το Google Docs και το Google Spreadsheet, οι οποίες παρουσιάζουν μεγάλο ενδιαφέρον κατά την διερεύνηση δικτύων. Οι περισσότερες εφαρμογές μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιούν μία μορφή javascript, συμπεριλαμβανομένων αυτές των Yahoo! και Microsoft οι οποίες προσφέρουν διαδικτυακές εφαρμογές μηνυμάτων ηλεκτρονικού ταχυδρομείου πλήρως υλοποιημένες σε AJAX.

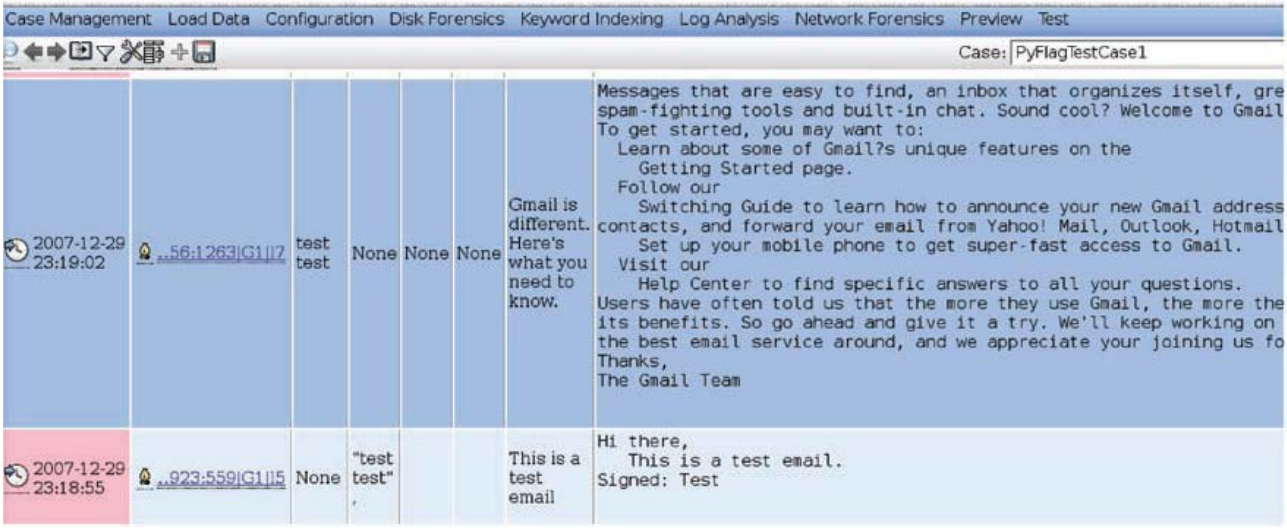
Παράδειγμα, το Gmail

Η πολυπλοκότητα των εφαρμογών διαδικτύου κάνουν δύσκολη την πιστή απόδοση τους. Για παράδειγμα, το Gmail έχει επαναπροσδιορίσει την έννοια των εφαρμογών διαδικτύου, οι οποίες παραδοσιακά αποτελούνταν από μία ακολουθία ιστοσελίδων HTML, που παράγονταν από τον διακομιστή ιστού. Το Gmail είναι καλύτερο να το σκεφθούμε ως μία εφαρμογή η οποία είναι γραμμένη σε javascript, εκτελείται στο τοπικό σύστημα, τρέχει στον περιηγητή ιστού, και χρησιμοποιεί αιτήσεις HTTP για να επικοινωνήσει με τον διακομιστή.

Όταν ένας χρήστης συνδεθεί με το Gmail, ο περιηγητής φορτώνει μία ασαφής εφαρμογή γραμμένη σε γλώσσα javascript. Μόλις η εφαρμογή εκκινήσει, στέλνει αιτήματα στο διακομιστή και ανακτά τα δεδομένα τα οποία απαιτούνται. Στη συνέχεια τα δεδομένα μεταδίδονται μέσω HTTP στους διακομιστές της Google με μία μοναδική και μη τεκμηριωμένη μορφοποίηση.

Ωστόσο, ο διερευνητής δικτύων στην πράξη ενδιαφέρεται λιγότερο για τον τρόπο με τον οποίο εμφανίζεται η εφαρμογή, αλλά για τις πληροφορίες υψηλού επιπέδου, όπως τα μηνύματα που εστάλησαν, λήφθηκαν και επεξεργάστηκαν. Αντίστοιχα, όταν γίνεται ανάλυση της κίνησης SMTP και POP, ο αναλυτής δεν ενδιαφέρεται για το μέσο το οποίο χρησιμοποιήθηκε για την αποστολή και την λήψη των μηνυμάτων, αλλά πως αυτά παρουσιάστηκαν στην οθόνη του χρήστη καθώς και αυτό καθαυτό το περιεχόμενο των μηνυμάτων.

Στην πραγματικότητα το Gmail είναι ένα μοναδικό πρωτόκολλο, το οποίο ανήκει στην Google, και εκτελείται πάνω στο επίπεδο του HTTP. Οι πληροφορίες της διερεύνησης μπορούν να εξαχθούν με αντίστροφη μηχανική του πρωτοκόλλου του Gmail. Ένα παράδειγμα ενός πακέτου εφαρμογών δικανικής δικτύων, η οποία υποστηρίζει την ανάλυση της κίνησης του Gmail είναι το PyFlag. Παρακάτω παρουσιάζονται τα μηνύματα ηλεκτρονικού ταχυδρομείου σε ένα πίνακα: (Li, 2010)



Εικόνα 9: Τα μηνύματα Gmail παρουσιάζονται σε ένα πίνακα. Το PyFlag δεν μπόρεσε να αποδώσει πιστά την ιστοσελίδα διότι είχε κατασκευαστεί δυναμικά στον περιηγητή ιστού του χρήστη. Όμως οι σημαντικές πληροφορίες συνοψίζονται σε αυτόν τον πίνακα. (Li, 2010)

3.10 Μέθοδοι καταγραφής της κίνησης δικτύου με τη χρήση υλικού

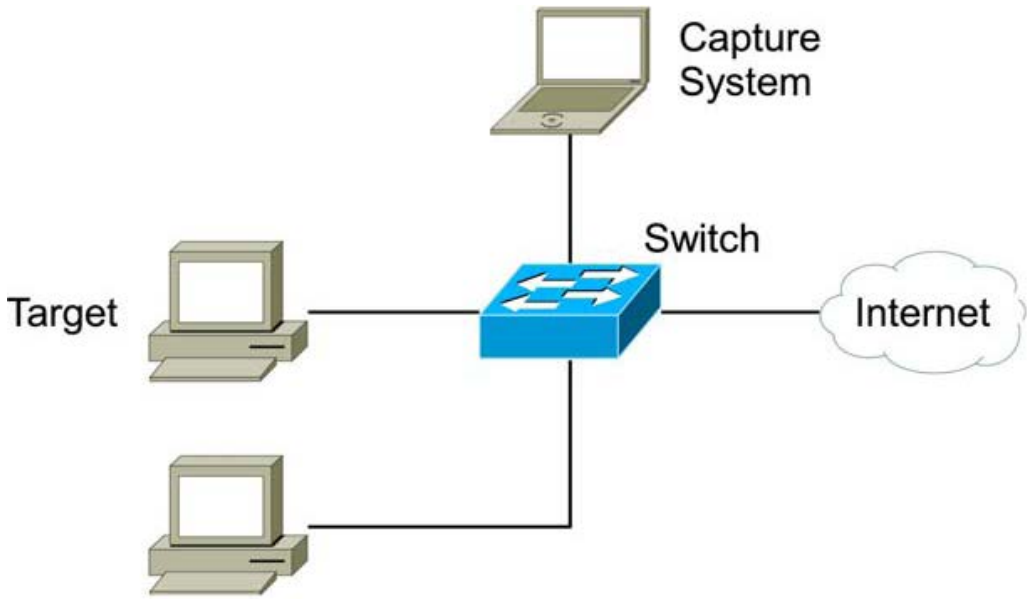
3.10.1 Ομφαλός (Repeater Hub)

Ένα repeater hub ή ομφαλός είναι μία συσκευή η οποία χρησιμοποιείται για να συνδέσει πολλά ζεύγη δικτυακών συσκευών, οι οποίες είναι διασυνδεδεμένες με ethernet. Η συσκευή λειτουργεί αναμεταδίδοντας όλα τα πλαίσια τα οποία λαμβάνει σε οποιαδήποτε από τις θύρες τις, σε όλες τις άλλες θύρες. Λόγω της λειτουργίας της αναμετάδοσης, με ένα σύστημα καταγραφής μπορούμε να λάβουμε όλη την κίνηση η οποία στέλνεται από οποιαδήποτε συσκευή στο τοπικό δίκτυο.

Επομένως οι ομφαλοί έχουν ευρεία κάλυψη, διότι επιτρέπουν σε ένα σύστημα καταγραφής να παρακολουθεί όλη την κίνηση από οποιαδήποτε συσκευή η οποία είναι συνδεδεμένη στον ομφαλό. Το γεγονός αυτό είναι ιδανικό από τη σκοπιά της διερεύνησης δικτύων. Βέβαια στην πράξη, είναι σπάνια η ευρεία χρήση των ομφαλών, και ακόμη πιο σπάνιο να λειτουργούν σε υψηλές ταχύτητες (άνω των 100mb/s). Οι ομφαλοί δεν λειτουργούν σε υψηλές ταχύτητες λόγω της χαμηλής ταχύτητα μεταγωγής.

3.10.2 Μεταγωγείς (Managed Switch) – Διασυνδεδεμένες Θύρες (Spanning Ports)

Η χρήση μεταγωγέων ethernet είναι συνηθέστερη. Ο μεταγωγέας είναι μία έξυπνη συσκευή η οποία λειτουργεί στο δεύτερο επίπεδο του δικτύου και προωθεί τα πακέτα στις θύρες για τις οποίες προορίζονται (δηλαδή βάσει της διεύθυνσης MAC). Αυτό επιτρέπει στις συσκευές οι οποίες είναι συνδεδεμένες με τον μεταγωγέα να επικοινωνούν χρησιμοποιώντας αποδοτικότερα το διαθέσιμο εύρος ζώνης.



Εικόνα 10: Ένα τυπικό δίκτυο ethernet συνδεδεμένο μέσω ενός μεταγωγέα (Li, 2010).

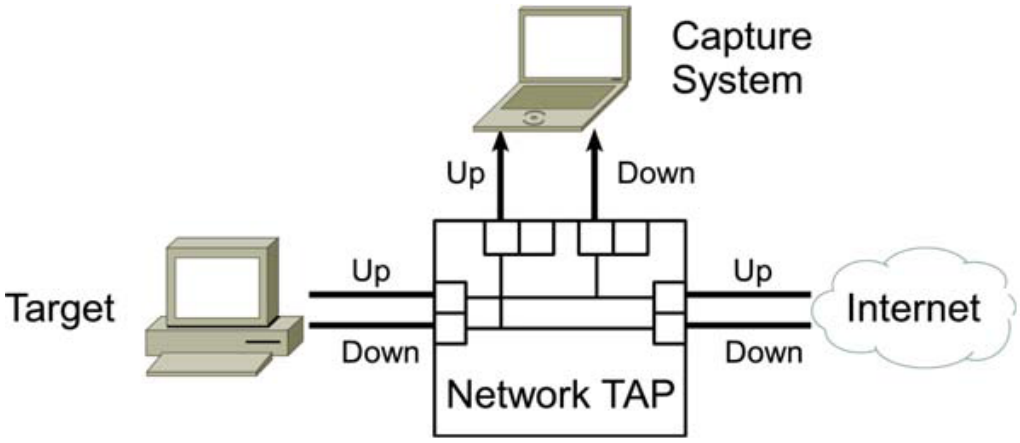
Στην παραπάνω εικόνα παρουσιάζεται ένα τυπικό σενάριο. Το σύστημα στόχος είναι συνδεδεμένο με ένα μεταγωγέα στο διαδίκτυο, καθώς επίσης και το σύστημα καταγραφής είναι συνδεδεμένο στον ίδιο μεταγωγέα. Κανονικά το σύστημα καταγραφής δεν μπορεί να παρακολουθήσει την διαδικτυακή κίνηση του συστήματος στόχου διότι τα πλαίσια αυτά δεν απευθύνονται στο σύστημα καταγραφής. Το σύστημα καταγραφής μπορεί να παρακολουθήσει μόνο τα πλαίσια αναμετάδοσης (όπως οι αιτήσεις ARP ή DHCP).

Ωστόσο, οι περισσότεροι μεταγωγείς έχουν την ικανότητα να δημιουργήσουν μία διασυνδεδεμένη θύρα. Η διασυνδεδεμένη θύρα είναι μία από τις φυσικές θύρες η οποία μπορεί να δημιουργηθεί ώστε να λάβει όλη την κίνηση δικτύου από ένα σύνολο θυρών Ethernet. επίσης μπορούν να ληφθούν κάποια ενεργά μέτρα, όπως παραποίηση ARP ή πλημμύρα MAC, ώστε η μεταγωγή της κίνησης δικτύου να σταλεί στη διεπαφή του συστήματος καταγραφής

Η τεχνική αυτή χρησιμοποιείται συνηθέστερα για την ανάπτυξη αισθητήρων IDS σε ένα επιχειρηματικό περιβάλλον. Με την μέθοδο αυτή, προσφέρεται μεγάλη επιλεκτικότητα διότι γίνεται διασύνδεση μόνο των θυρών του συστήματος στόχου. Ωστόσο, όπως και στην μέθοδο του ομφαλού, η διασυνδεδεμένη κίνηση δικτύου συγκεντρώνεται στο ίδιο τμήμα του ethernet οδηγώντας σε πιθανές συγκρούσεις και απώλεια πακέτων. Το γεγονός αυτό είναι ιδιαίτερα σημαντικό διότι στην περίπτωση που χρησιμοποιείται διπλό ethernet, τόσο τα δεδομένα που ανεβαίνουν όσο και αυτά που κατεβαίνουν συγκεντρώνονται στην θύρα του συστήματος καταγραφής.

3.10.3 Χρησιμοποιώντας ένα δίκτυο TAP

Τα δίκτυα TAP είναι συσκευές ειδικά σχεδιασμένες ώστε να επιτρέπουν την παρεμβολή μεταξύ δύο συσκευών ethernet. Το σύστημα στόχου συνδέεται στο TAP με μία διπλή σύνδεση η μία χρησιμοποιείται για τα δεδομένα ανόδου και η δεύτερη για τα δεδομένα καθόδου. Το TAP διαχωρίζει αυτήν την σύνδεση σε δύο διαφορετικές φυσικές θύρες ethernet, εκ των οποίων η καθεμία λαμβάνει μόνο μία πλευρά της σύνδεσης. Με την αρχιτεκτονική αυτή είναι δυνατή η καταγραφή της κίνησης που κατεβαίνει και ανεβαίνει χωρίς να υπάρχει απώλεια πακέτων (Li, 2010).



Εικόνα 11: Ένα δίκτυο TAP (Li, 2010)

4. Εργαλεία της Δικανικής Δικτύων

Έχουν αναπτυχθεί αρκετά εργαλεία για την εκτέλεση εργασιών συστηματικής διερεύνησης δικτύων υπολογιστών όπως τα Snort και TcpDump. Η κατηγοριοποίηση τους μπορεί να γίνει με δύο τρόπους:

1ος τρόπος κατηγοριοποίησης

Σύμφωνα με τον πρώτο τρόπο κατηγοριοποίησης ανήκουν τρεις κατηγορίες εργαλείων:

1. Τα εργαλεία που εμπίπτουν στην κατηγορία αυτή είναι τα συστήματα ανίχνευσης παρείσφρησης, όπως το Snort. Τα εργαλεία αυτά είναι χρήσιμα σε περιπτώσεις μίας γρήγορης στατιστικής επισκόπησης της καταγεγραμμένης κίνησης και ανίχνευσης των προφανών προτύπων επίθεσης.
2. Τα εργαλεία που εμπίπτουν στην κατηγορία αυτή είναι τα εργαλεία διάγνωσης δικτύου, όπως το Wireshark, το οποίο παρέχει λεπτομερή διχοτόμηση των πρωτοκόλλων και υποστήριξη για ένα μεγάλο αριθμό πρωτοκόλλων. Ωστόσο τα εργαλεία αυτά δεν έχουν σχεδιαστεί με γνώμονα τον μεγάλο όγκο των δεδομένων που καλούνται να αντιμετωπίσουν κατά την διερεύνηση δικτύων. Βέβαια διατηρούν την χρησιμότητά τους για την εξέταση ενός μικρού υποσυνόλου της κίνησης δικτύου.
3. Τα εργαλεία που εμπίπτουν στην κατηγορία αυτή είναι τα εργαλεία δικανικής δικτύων τα

οποία έχουν σχεδιαστεί ειδικά για την ανάλυση των δικτυακών δεδομένων, όπως το PyFlag. Αυτά τα εργαλεία είναι σχεδιασμένα ώστε να διαχειρίζονται τον όγκο των δεδομένων που συναντούν και παρουσιάζουν στον αναλυτή πληροφορίες υψηλού επιπέδου, όπως μηνύματα ηλεκτρονικού ταχυδρομείου και ιστοσελίδες, πληροφορίες δηλαδή για τις οποίες ενδιαφέρονται περισσότερο οι αναλυτές δικτύων. Αυτά τα εργαλεία συνήθως δεν υποστηρίζουν τόσα πολλά πρωτοκολλά όπως τα εργαλεία διάγνωσης δικτύου, αλλά επικεντρώνονται στα πρωτόκολλα που διαδραματίζουν τον πιο σημαντικό ρόλο στην διερεύνηση δικτύων (Li, 2010).

2ος τρόπος κατηγοριοποίησης

Σύμφωνα με τον δεύτερο τρόπο κατηγοριοποίησης των εργαλείων συστηματικής διερεύνησης δικτύων υπολογιστών, τα εργαλεία αυτά μπορούν να διαχωριστούν με βάση τα συστήματα στα οποία γίνεται η διερεύνηση, δηλαδή στα τερματικά συστήματα και στα δίκτυα υπολογιστών. Τα εργαλεία τα οποία βασίζονται στα τερματικά συστήματα, εξετάζουν τα εισερχόμενα πακέτα σε ένα συγκεκριμένο τερματικό και παρουσιάζουν στον αναλυτή δικτύων στατιστικά δεδομένα σχετικά με την κίνηση δικτύου σε αυτό το τερματικό σύστημα. Από την άλλη πλευρά, τα εργαλεία τα οποία βασίζονται σε δίκτυα υπολογιστών, έχουν πολλαπλά συστήματα που κατοικοεδρεύουν σε διαφορετικά μέρη του δικτύου και επικοινωνούν μεταξύ τους, ούτως ώστε να παρουσιάσουν πληροφορίες από την μεριά ενός δικτύου υπολογιστών. Στην συνέχεια γίνεται σύντομη παρουσίαση των διαθέσιμων εργαλείων συστηματικής διερεύνησης δικτύων υπολογιστών που εμπίπτουν στις δύο αυτές κατηγορίες (Kanellis, 2006).

4.1 Εργαλεία που βασίζονται σε τερματικά συστήματα

Τα εργαλεία συστηματικής διερεύνησης δικτύων υπολογιστών που βασίζονται σε τερματικά συστήματα, εκτελούνται σε ένα τερματικό σύστημα στο δίκτυο και βοηθούν στην κατανόηση των λειτουργιών του δικτύου, συλλέγοντας και αναλύοντας τα εισερχόμενα πακέτα του τερματικού συστήματος. Τα αυτά εργαλεία παρέχουν πλήθος πληροφοριών, σε μορφή αρχείων καταγραφής τα οποία στη συνέχεια θα αναλυθούν από τον χρήστη.

4.1.1 Ethereal

Το Ethereal είναι ένα πρόγραμμα ανοικτού κώδικα το οποίο χρησιμοποιείται ευρέως ως αναλυτής πακέτων δικτύου. Καταγραφεί τα πακέτα που στέλνονται και λαμβάνονται σε ένα δίκτυο. Παρουσιάζει τις πληροφορίες των κεφαλίδων όλων των πρωτοκόλλων που χρησιμοποιούνται κατά την μετάδοση των πακέτων που καταγράφονται και φιλτράρει τα πακέτα βάσει των αναγκών του χρήστη (Meghanathan, 2009).

4.1.2 Wireshark

Το Wireshark είναι ένας ισχυρός αναλυτής πρωτοκόλλων δικτύου. Αρχικά ονομαζόταν Ethereal. Εκτελείται σε διάφορα λειτουργικά συστήματα συμπεριλαμβανομένων των Linux, Mac OS X, BSD, Solaris και Microsoft Windows. Η υλοποίηση του περιλαμβάνει μία γραφική διεπιφάνεια χρήστη και χρησιμοποιεί το pcap για την καταγραφή πακέτων.

Το Wireshark εμφανίζει την ενθυλάκωση και τα πεδία των διαφόρων πακέτων τα οποία προσδιορίζονται από διάφορα πρωτόκολλα δικτύωσης. Η βασική μορφή αρχείων που υποστηρίζει το Wireshark είναι η μορφή libpcap, οπότε μπορούν να εισαχθούν δεδομένα από άλλες εφαρμογές όπως το tcpdump. (Garrlson C., 2010)

4.1.3 TcpDump

Το TcpDump είναι ένα εργαλείο γραμμής εντολών τα οποίο χρησιμοποιείται για παρακολούθηση του δικτύου, αποσφαλμάτωση πρωτοκόλλων και απόκτηση των δεδομένων δικτύου. Το TcpDump εμφανίζει τις κεφαλίδες των πακέτων σε μία διεπαφή δικτύου, οι οποίες ταιριάζουν με μία δοσμένη λογική έκφραση. Το εργαλείο αυτό διατίθεται για διάφορες πλατφόρμες και καταγράφει τα δεδομένα σε μορφή αρχείου pcap. Στην έκδοση του για Windows, η οποία ονομάζεται WinDump, το εργαλείο λαμβάνει όλα τα εισερχόμενα πακέτα, χωρίς να κάνει διαχωρισμό των πακέτων. Το tcpdump εκτελείται συνήθως σε ένα διαμεριζόμενο δίκτυο, ούτως ώστε να μπορεί να παρακολουθήσει την κίνηση δικτύου και σε άλλα τερματικά (Kanellis, 2006).

Όσον αφορά τη χρήση του tcpdump, το εργαλείο αυτό μπορεί να καταγράψει την κίνηση δικτύου χρησιμοποιώντας φίλτρα ούτως ώστε να περιορίσουμε τον αριθμό των συνδέσεων για τις οποίες ενδιαφερόμαστε. Για παράδειγμα, εάν υπάρχει απαίτηση για καταγραφή της κίνησης του πρωτοκόλλου HTTP για αρχεία μεγαλύτερα των 100MB, το γεγονός αυτό επιτυγχάνεται με την παρακάτω εντολή:

```
/sbin/tcpdump -C 100 -s 0 -w output.pcap port 80
```

Να σημειώσουμε ότι χρησιμοποιούμε την παράμετρο “-s 0” ώστε να εξασφαλιστεί ότι το πλήρες πακέτο καταγράφεται στο αρχείο εξόδου. Προεπιλεγμένα το tcpdump καταγράφει μόνο 64 bytes από την αρχή του κάθε πλαισίου. Για να περιορίσουμε την καταγραφή μόνο των πακέτων που έχουν ως πηγή ή ως προορισμό την θύρα 80, χρησιμοποιείται η παράμετρος “port 80” (Li, 2010).

4.1.4 Xprobe2

Το Xprobe2 είναι ένα δυναμικό εργαλείο απομακρυσμένης αναζήτησης ιχνών σε λειτουργικά συστήματα το οποίο έχει διαφορετική προσέγγιση από άλλα παρόμοια λογισμικά. Το Xprobe2 στηρίζεται σε ένα ασαφές ταίριασμα υπογραφών, υποθέσεις πιθανοτήτων, και μία βάση δεδομένων υπογραφών.

Περιλαμβάνει:

- Ένα εργαλείο ανίχνευσης TCP
- Ένα ανιχνευτή θυρών
- Αυτόματο έλεγχο λήξης χρόνου για τα διάφορα εργαλεία του Xprobe2
- Δυνατότητα πλήρη ελέγχου όλων των λειτουργιών του
- Μία βάση δεδομένων υπογραφών με πάνω από 160 υπογραφές

Το Xprobe2 λειτουργεί εφαρμόζοντας στατιστική ανάλυση βασισμένη σε ένα μαθηματικό αλγόριθμο παρέχοντας το καλύτερο δυνατό ταίριασμα μεταξύ των δεδομένων που λήφθηκαν από το σύστημα στόχο και τη βάση δεδομένων υπογραφών. Ακόμη χρησιμοποίει μία απλή μορφή λογισμικού οπτικής αναπαράστασης χαρακτήρων (OCR), χρησιμοποιώντας ένα πίνακα βασισμένο στα ίχνη που ταιριάζουν και σε στατιστικό υπολογισμό των αποτελεσμάτων κάθε ελέγχου που διενεργήθηκε. Η προσέγγιση της ασαφής λογικής, παρέχει καλύτερη αντίσταση σε επιδράσεις του περιβάλλοντος. (Arkin O., 2003)

4.1.5 Snort

Το Snort είναι εργαλείο ασφάλειας δικτύων ανοικτού κώδικα το οποίο αρχικά αναπτύχθηκε για την πλατφόρμα Unix το 1998 και στη συνέχεια υλοποιήθηκε για συστήματα Windows. Το Snort είναι ένα απλό εργαλείο γραμμής κώδικα το οποίο χρησιμοποιείται για την παρακολούθηση της κίνησης δικτύου. Το Snort χρησιμοποιεί κανόνες βάσει των οποίων εκτελεί αναζήτηση για υπογραφές παραβίασης του συστήματος. Όταν γίνει ταίριασμα ενός κανόνα ειδοποιεί τον χρήστη και εισάγει μία καταχώρηση στο αρχείο καταγραφής. Αναλύει πρωτοκόλλα, επιδιορθώνει το δίκτυο, και ελέγχει τις μη εξουσιοδοτημένες εφαρμογές. Το Snort χρησιμοποίει μικρό χώρο μνήμης και απαιτεί πολύ μικρή επεξεργαστική ισχύ. Το Snort μπορεί να παρακολουθεί όλη την κίνηση σε έναν υπολογιστή ή μπορεί να τοποθετηθεί σε ένα προσαρμογέα δικτύου ώστε να παρακολουθεί όλη την κίνηση πάνω στην διασύνδεση.

4.1.6 Argus

Το Argus είναι ένα λογισμικό ανοικτού κώδικα το οποίο παρακολουθεί τη δραστηριότητα δικτύου. Εξετάζει το δίκτυο βάσει του πρωτοκόλλου IP, παρακολουθεί και καταγράφει πληροφορίες της κίνησης δικτύου, δημιουργεί αρχεία καταγραφής ώστε να επιλυθούν προβλήματα του δικτύου και να επαληθευτεί ότι λειτουργούν οι πολιτικές ασφάλειες του δικτύου.

Το Argus είναι διαθέσιμο για διάφορες πλατφόρμες UNIX συμπεριλαμβανομένων των Solaris, IRIX, FreeBSD, OpenBSD, NetBSD, και Linux. (Tullock M., 2003)

4.1.7 Netstat

Το Netstat είναι μία βασική εντολή η οποία ενσωματώνεται στις περισσότερες εκδόσεις των Unix και των Windows. Παρουσιάζει στατιστικά στοιχεία χρήσης του δικτύου και πληροφορίες δρομολόγησης καθώς και μία λίστα των συνδέσεων TCP και UDP από και προς τον υπολογιστή, δηλαδή αυτές που εγκαθιδρύθηκαν ή περιμένουν να εγκαθιδρυθούν ή έκλεισαν πρόσφατα. Επίσης παρουσιάζεται η διεύθυνση IP κάθε απομακρυσμένου υπολογιστή με τον οποίο γίνεται επικοινωνία. (Casey E., 2003)

4.1.8 Fiddler

Το Fiddler είχε αναπτυχθεί από την Microsoft για να καταπολεμήσει τα ενοχλητικά μηνύματα των μηχανών αναζήτησης. Το Fiddler είναι ένας τοπικός διακομιστής proxy, ο οποίος επιτρέπει στον ερευνητή να συλλέξει όλη τη κίνηση ιστού των πρωτοκόλλων http, https και ftp. Το Fiddler αποκαλύπτει όλες τις παρεμβαλλόμενες ιστοσελίδες μέχρι την ιστοσελίδα προορισμού. Όλα τα ύποπτα λογισμικά που παραλείφθηκε θα αποκαλυφθούν και θα ληφθούν. Όλες οι ιστοσελίδες που επισκεφθήκαμε καταγράφονται σε ένα αρχείο καταγραφής της συνόδου καθώς και οι ληφθείσες εφαρμογές και οι ανακατευθύνσεις σε άλλες ιστοσελίδες. Το Fiddler ενσωματώνει διάφορα εργαλεία τα οποία εξάγουν πληροφορίες με διάφορους τρόπους. (Garrlson C., 2010)

4.1.9 NTLast

Το εργαλείο NTLast είναι ένα πολύ καλό εργαλείο το οποίο επιτρέπει την παρακολούθηση των επιτυχημένων και αποτυχημένων προσπαθειών σύνδεσης στο σύστημα. Το εργαλείο αυτό είναι χρήσιμο μόνο σε περιπτώσεις που έχει ενεργοποιηθεί στο σύστημα η κατάλληλη πολιτική. Χρησιμοποιώντας το εργαλείο αυτό μπορούμε να αναζητήσουμε για ύποπτους λογαριασμούς χρήστη και απομακρυσμένα συστήματα τα οποία συνδέθηκαν στο σύστημα στόχο. (Promise C., 2003)

4.1.10 p0f

Το p0f είναι ένα ευέλικτο παθητικό εργαλείων ανίχνευσης λειτουργικών συστημάτων. Το p0f μπορεί να ανιχνεύσει μηχανήματα τα οποία συνδέονται με το σύστημα στόχο, συστήματα στα οποία συνδέεται το σύστημα στόχος, και συσκευές οι οποίες βρίσκονται πίσω από ένα πακέτο που λήφθηκε. Ακόμη μπορεί να εντοπίσει το φυσικό μέσο με το οποίο είναι συνδεδεμένο το απομακρυσμένο σύστημα, την απόσταση στην οποία βρίσκεται και το χρόνο που είναι σε λειτουργία. Το p0f εντοπίζεται το απομακρυσμένο σύστημα εξετάζοντας διάφορα πεδία στην διεύθυνση IP και τις κεφαλίδες TCP του TCP SYN ή τα πακέτα SYN/ACK τα οποία προέρχονται από το απομακρυσμένο σύστημα.

4.1.11 Fport

Το Fport είναι ένα εργαλείο για συστήματα Windows το οποίο παρουσιάζει όλες τις ανοικτές θύρες TCP/IP και UDP, και αναθέτει τις εφαρμογές οι οποίες αντιστοιχούν στην κάθε θύρα. Ακόμη αναθέτει σε αυτές τις θύρες τις εκτελούμενες διεργασίες με το αναγνωριστικό τους, το όνομα και τη διαδρομή που βρίσκεται η εφαρμογή. Το Fport μπορεί να ανιχνεύσει ταχύτητα άγνωστες ανοικτές θύρες και να τις αντιστοιχίσει σε εφαρμογές. (Schweitzer D., 2003)

4.2 Εργαλεία που βασίζονται σε δίκτυα υπολογιστών

Τα εργαλεία συστηματικής διερεύνησης δικτύων που βασίζονται σε δίκτυα υπολογιστών αποτελούνται από πολλαπλά σημεία παρακολούθησης και μπορούν να τοποθετηθούν σε διαφορετικά σημεία του δικτύου και να χρησιμοποιηθούν για κατανεμημένη παρακολούθηση του δικτύου. Για να εκτελεστούν ορισμένες εργασίες συστηματικής διερεύνησης δικτύων όπως το IP traceback, η αναδημιουργία της επίθεσης ή η ιχνηλάτιση ηλεκτρονικού ταχυδρομείου οι απαιτούμενες πληροφορίες θα πρέπει να συλλεχθούν από τερματικά συστήματα στο ίδιο δίκτυο με

το σύστημα όπου έγινε η επίθεση, ή από συνεργαζόμενα ή εχθρικά μέρη ως προς το σύστημα όπου έγινε η επίθεση. Τέτοιου είδους εργαλεία παρακολούθησης δικτύου ενοποιούν τα δεδομένα από διαφορετικά σημεία παρακολούθησης και παρέχουν μία πλήρη και ολοκληρωμένη άποψη της κίνησης δικτύου. Παρακάτω αναλύονται τα κύρια σημεία εργαλείων συστηματικής διερεύνησης δικτύων με υλοποίηση σε επίπεδο δικτύου.

4.2.1 Niksun NetDetector

Το NetDetector είναι ένα πακέτο εφαρμογών το οποίο χρησιμοποιείται για παρακολούθηση της ασφάλειας στο δίκτυο, ανίχνευση, ανάλυση και συστηματική διερεύνηση. Λειτουργεί ελέγχοντας τις υπογραφές των αρχείων, ανιχνεύει ανωμαλίες με στατιστικές μεθόδους και καταγράφει και αποθηκεύει όλα τα γεγονότα δικτύου. Συνοδεύεται από μία ισχυρή διεπιφάνεια χρήστη, και έχει την δυνατότητα εξελιγμένης αναδημιουργίας ιστοσελίδων, μηνυμάτων ηλεκτρονικού ταχυδρομείου, άμεσων μηνυμάτων, συνδέσεων FTP και Telnet, εφαρμογών VoIP, και αναλύει το δίκτυο σε επίπεδο πακέτων. Επίσης μπορεί να ενσωματωθεί με τα προϊόντα Cisco IDS, Micromuse NetCool, και το IBM/Tivoli Risk Manager. Οι συσκευές που το χρησιμοποιούν μπορούν να είναι κατανεμημένες σε διάφορα σημεία ενός οργανισμού και κατόπιν γίνεται η διαχείρισή τους από ένα κεντρικό σημείο του οργανισμού, παρέχοντας στο αναλυτή αναφορές και ανάλυση του δικτύου του οργανισμού. (Kanellis, 2006)

4.2.2 Niksun NetIntercept

Το NetIntercept βοηθά στην κατανόηση της κίνησης στο δίκτυο και στην αναγνώριση εισβολών στο δίκτυο. Έχει την δυνατότητα να ανασυνθέσει τα πακέτα ως ροές δεδομένων και να ανιχνεύσει και να αναλύσει το περιεχόμενο ηλεκτρονικών μηνυμάτων, ιστοσελίδων και αρχείων. Το NetIntercept προσφέρει απομακρυσμένη διαχείριση και αποκρυπτογράφηση SSH2 μέσω τροποποιημένων διακομιστών. Οι αναλυτές μπορούν να δουν πληροφορίες σε επίπεδο σύνδεσης, να καταγράψουν μία κεφαλίδα ή κάποια προσπάθεια παραποίησης μίας θύρας επικοινωνίας για κάποια άλλη. Μπορούν να αποκαλυφθούν κωδικοί καθαρού κειμένου, και τα περιεχόμενα μιας μη κρυπτογραφημένης εξ αποστάσεως σύνδεσης. Είναι πολύ χρήσιμο εργαλείο για την μελέτη εξωτερικών προσπαθειών

παρείσφρησης και είναι ικανό να αναλύσει εκατοντάδες χιλιάδες διαδικτυακές συνδέσεις.

4.2.3 Pcap

Η βιβλιοθήκη Packet Capture παρέχει μία διεπιφάνεια υψηλού επιπέδου για να καταγραφούν και αναλυθούν τα πακέτα στο δίκτυο. Η βιβλιοθήκη Pcap αποτελεί την βάση για πολλές εφαρμογές παρακολούθησης δικτύου του Unix. Η βιβλιοθήκη Pcap χρησιμοποιεί ένα σετ εντολών του Unix οι οποίες είναι γνωστές ως Berkley Packet Filter (BPF). Το WinPcap αποτελεί την έκδοση του Pcap για Windows και αποτελείται από δύο κύρια συστατικά, τον οδηγό προγράμματος ο οποίος παρέχει στο σύστημα πρόσβαση χαμηλού επιπέδου δικτύωσης, και μία βιβλιοθήκη η οποία παρέχει έυκολη πρόσβαση στα χαμηλά επίπεδα δικτύωσης. Με το πρόγραμμα οδήγησης προστίθεται η δυνατότητα συλλογής και αποστολής πακέτων μέσω δικτύου για τα συστήματα Windows με παρόμοιο τρόπο όπως το BPF για συστήματα Unix.

4.2.4 SiLK

Το SiLK, είναι μία συλλογή εργαλείων ανάλυσης κίνησης τα οποία έχουν αναπτυχθεί για να διευκολύνουν την ανάλυση ασφάλειας μεγάλων δικτύων. Η σουίτα εργαλείων του SiLK υποστηρίζει την συλλογή, αποθήκευση και ανάλυση, δεδομένων ροής δικτύου, επιτρέποντας στους αναλυτές ασφάλειας δικτύου να εκτελούν ερωτήματα σε μεγάλα σύνολα δεδομένων. Το SiLK μπορεί να αναλύσει την κίνηση στα άκρα ενός μεγάλου και κατανεμημένου ISP ή σε ένα ISP μεσαίου μεγέθους.

Το SiLK περιλαμβάνει δύο κατηγορίες εφαρμογών, τις εφαρμογές συλλογής και τις εφαρμογές ανάλυσης. Τα προγράμματα συλλογής συλλέγουν ροές δεδομένων IPFIX, NetFlow v9, ή NetFlow v5, στη συνέχεια μετατρέπουν αυτές τις ροές σε αποδοτικότερη μορφοποίηση, και κατόπιν μετατρέπουν τις ροές σε δυαδικά αρχεία. Τα προγράμματα ανάλυσης περιλαμβάνουν εργαλεία, τα οποία διαβάζουν τα αρχεία, που παράχθηκαν προηγουμένως, και εκτελούν διάφορες διαδικασίες ερωτημάτων, οι οποίες περιλαμβάνουν στατιστική ανάλυση ομάδων εγγραφών και άλλες μεθόδους.

4.2.5 Nmap

Το Nmap είναι ένα εργαλείο ανοικτού κώδικα το οποίο χρησιμοποιείται από διαχειριστές δικτύου και επαγγελματίες ασφάλειας συστημάτων για να εξετάσουν επιχειρηματικά δίκτυα, αναζητώντας ενεργά τερματικά συστήματα, συγκεκριμένες υπηρεσίες ή λειτουργικά συστήματα. Το Nmap έχει την ικανότητα να δημιουργεί πακέτα IP και να τα στέλνει υλοποιώντας μοναδικές μεθοδολογίες εκτέλεσης των παραπάνω διερευνήσεων. Το Nmap λειτουργεί τόσο σε γραμμή εντολών όσο και σε γραφικό περιβάλλον και εγκαθίσταται τόσο σε συστήματα Unix, Windows όσο και σε Mac OS X. (Orebaugh A., 2008)

4.2.6 PyFlag

Το εργαλείο PyFlag είναι ένα ανεπτυγμένο εργαλείο ανάλυσης αρχείων καταγραφής μεγάλο όγκου όπως αντίγραφα σκληρών δίσκων και αρχεία καταγραφών δικτύου. Μεταξύ άλλων το PyFlag χρησιμοποιείται σε διάφορους κλάδους της ψηφιακής δικανικής συμπεριλαμβανομένης και της δικανικής δικτύων. Το PyFlag είναι ικανό να αναλύσει αρχεία καταγραφής δικτύου μορφοποίησης του tcpdump και υποστηρίζει μεγάλο αριθμό δικτυακών πρωτοκόλλων. Είναι ικανό να εξάγει πληροφορίες υψηλού επιπέδου και να εντοπίσει με ακρίβεια από πού εξάχθηκε κάθε κομμάτι δεδομένων. Η αρχιτεκτονική του PyFlag είναι υλοποιημένη ώστε τα δεδομένα να εξετάζονται αναδρομικά σε πολλαπλά επίπεδα, γεγονός το οποίο είναι ιδανικό για τα πρωτόκολλα δικτύου τα είναι στρωματοποιημένα με τέτοιο τρόπο ώστε τα υψηλότερα επίπεδα πρωτοκόλλων να μεταφέρονται από τα χαμηλότερα επίπεδα.

Τα βασικά συστατικά του εργαλείου αυτού είναι η αναδημιουργία ροής, ο χειριστής πακέτων και η διχοτόμηση των ροών δεδομένων. Το PyFlag δέχεται ως εισαγωγή αρχεία pcap, εξάγει τα πακέτα και τα διχοτομεί σε χαμηλότερα επίπεδα πρωτοκόλλων (IP, TCP ή UDP). Τα συσχετιζόμενα πακέτα συλλέγονται σε ροές χρησιμοποιώντας την αναδημιουργία ροής. Αυτές οι ροές στη συνέχεια διχοτομούνται σε υψηλότερα επίπεδα πρωτοκόλλων (HTTP, IRC και άλλα). Το PyFlag αναδημιουργεί συνόδους HTTP και είναι ικανό να διχοτομήσει εφαρμογές υψηλού επιπέδου όπως εφαρμογές ηλεκτρονικού ταχυδρομείου. Το PyFlag διαχειρίζεται κάθε περίπτωση ξεχωριστά και

χρησιμοποιεί μία μοναδική ταυτότητα για κάθε είσοδο και έξοδο δεδομένων. Αναγνωρίζει τους τύπους των αρχείων και παρουσιάζει το εικονικό σύστημα αρχείων σε μορφή δέντρου. Επίσης παρουσιάζεται η κίνηση μεταξύ διαφόρων πηγών και προορισμών και προς τις δύο κατευθύνσεις. Γίνεται επισκόπηση των περιεχομένων κάθε πακέτου και πρωτοκόλλου. Τέλος γίνεται επισκόπηση και ανάλυση των συνδέσεων που εγκαθιδρύθηκαν, των συνομιλιών και των αιτήσεων DNS. (Pilli E.,2010)

4.2.7 Raytheon SilentRunner

Το SilentRunner παρέχει μία τρισδιάστατη άποψη του δικτύου. Επικεντρώνεται στην παρακολούθηση δικτύου και ανάλυση, οπότε εάν ανιχνευθεί ασυνήθης κίνηση στο δίκτυο δημιουργούνται προειδοποιήσεις. Ακόμη παρέχεται παρακολούθηση των πακέτων που διασχίζουν το δίκτυο. Το εργαλείο παρέχει επίσης την δυνατότητα επανάληψης των γεγονότων όπως αυτά συνέβησαν. Βάσει των μοτίβων της κίνησης δικτύου που παράγονται οι διερευνητές δικτύου μπορούν να βοηθηθούν για να αποκτήσουν αποδεικτικά στοιχεία για ένα συγκεκριμένο γεγονός. (Sira R., 2003)

4.2.8 NetWitness Investigator

Το NetWitness Investigator είναι ένα εργαλείο που έχει την ικανότητα να καταγράψει την κίνηση δικτύου, να αναδημιουργήσει συνόδους, να παρουσιάσει σε πραγματικό χρόνο περιεχόμενο όπως αυτό παρουσιάστηκε, και να αναλύσει την κίνηση με πολλούς τρόπους ακόμη και σε πραγματικό χρόνο.

4.2.9 Bro

Το Bro είναι ένα εργαλείο ανοικτού κώδικα που παρακολουθεί παθητικά την κίνηση δικτύου και ελέγχει για ύποπτη δραστηριότητα. Το Bro ανιχνεύει τις εισβολές εισάγοντας πρώτα την κίνηση δικτύου για να εξάγει πληροφορίες σε επίπεδο εφαρμογής και στη συνέχεια εκτελεί αναλύσεις σχετικά με γεγονότα και συγκρίνει τη δραστηριότητα αυτή με μοτίβα, ώστε να κριθεί εάν η δραστηριότητα αυτή είναι ύποπτη. Η ανάλυση περιλαμβάνει ανίχνευση συγκεκριμένων επιθέσεων και ασυνήθιστες δραστηριότητες.

Το Bro χρησιμοποιεί μια εξειδικευμένη γλώσσα πολιτικών ασφάλειας, η οποία καθοδηγεί τη λειτουργία του. Εάν ανιχνευθεί κάποια ύποπτη δραστηριότητα, είτε δημιουργείται μία καταχώρηση στο αρχείο καταγραφής είτε ειδοποιείται ο ερευνητής σε πραγματικό χρόνο, είτε εκτελείται μία εντολή του λειτουργικού συστήματος. Επομένως το Bro είναι αρκετά χρήσιμο για την δικανική δικτύων.

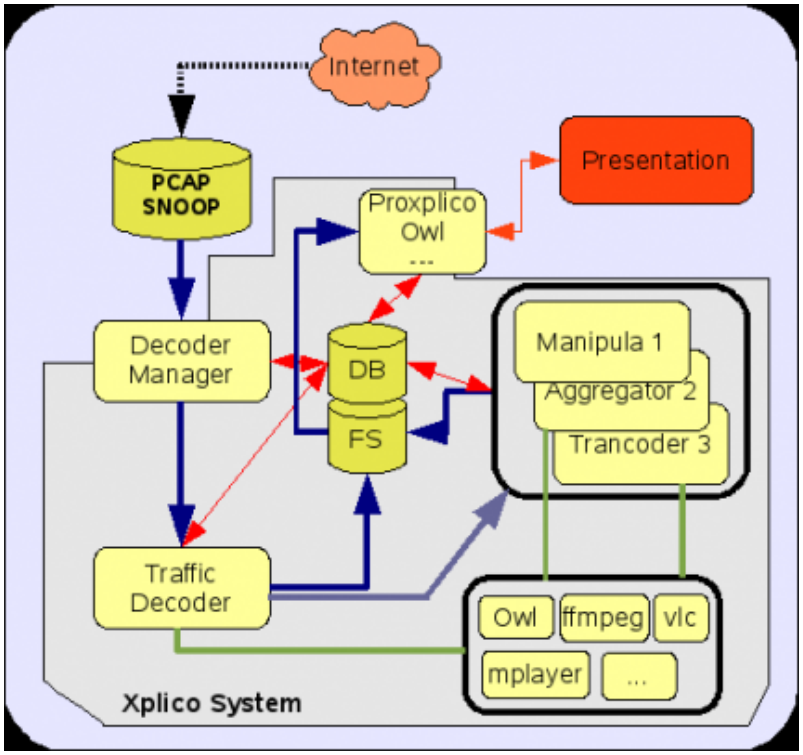
4.2.10 Ettercap

Το Ettercap σχεδιάστηκε για την παρακολούθηση δικτύων. Έχει ενσωματωμένες λειτουργίες για συλλογή συνθηματικών χρήστη, ανίχνευση λειτουργικών συστημάτων και παθητική ή δυναμική διχοτόμηση πολλών πρωτοκόλλων.

4.2.11 Xplico

Το xplico είναι ένα εργαλείο ανάλυσης της δικανικής δικτύων. Η κύρια εργασία του Xplico είναι η εξαγωγή δεδομένων από μία καταγραφή δικτύου (είτε ένα από ένα αρχείο .pcap είτε κάνοντας καταγραφή σε πραγματικό χρόνο). Το Xplico αποτελείται από τέσσερα υποσυστήματα, ένα

διαχειριστή αποκωδικοποίησης ο οποίος λέγεται Dema, ένα αποκωδικοποιητή δικτύου και IP οποίος ονομάζεται xplico, ένα σύνολο εφαρμογών οι οποίες διαχειρίζονται τα αποκωδικοποιημένα δεδομένα και ένα σύστημα οπτικοποίησης για να παρουσιαστούν τα εξαγόμενα δεδομένα. (http://www.xplico.org/)



Εικόνα 12: Αρχιτεκτονική του εργαλείου Xplico (http://www.xplico.org/)

4.3 Εργαλεία ανάλυσης μηνυμάτων ηλεκτρονικού ταχυδρομείου

Τα εργαλεία που περιγράφονται σε αυτό το κεφάλαιο βοηθούν στην ταυτοποίηση της πηγής του μηνύματος, ανίχνευση της διαδρομής του μηνύματος και επίσης να ανιχνευθούν μηνύματα ηλεκτρονικού ταχυδρομείου που προσπαθούν να αποκτήσουν εμπιστευτικές πληροφορίες από τον λήπτη του μηνύματος.

4.3.1 eMailTrackerPro

Το eMailTrackerPro αναλύει την κεφαλίδα ενός μηνύματος ώστε να ανιχνευθεί η διεύθυνση IP του μηχανήματος από το οποίο εστάλη το μήνυμα και να αναγνωριστεί ο αποστολέας. Η κεφαλίδα των μηνυμάτων παρέχει έλεγχο της διαδρομής όλων των μηχανημάτων από όπου πέρασε το μήνυμα. Η βάση δεδομένων του eMailTrackerPro βοηθά στον εντοπισμό μηνυμάτων ηλεκτρονικού ταχυδρομείου σε μία χώρα ή περιοχή στον κόσμο, παρουσιάζοντας πληροφορίες σε ένα παγκόσμιο χάρτη. Το eMailTrackerPro παρέχει μία συνοπτική αναφορά η οποία περιέχει κρίσιμες πληροφορίες, οι οποίες μπορεί να φανούν χρήσιμες για την ανάλυση και διερεύνηση δικτύων. Η αναφορά που εξάγει το εργαλείο αυτό περιλαμβάνει την γεωγραφική τοποθεσία της διεύθυνσης IP από την οποία απεστάλη το μήνυμα ηλεκτρονικού ταχυδρομείου, και εάν δε μπορεί να βρεθεί, η αναφορά περιλαμβάνει την τοποθεσία του ISP. Επίσης η αναφορά περιλαμβάνει πληροφορίες για τον ιδιοκτήτη του δικτύου ή του ISP.

4.4 Εργαλεία περιηγητών ιστού

Οι κυρίαρχοι περιηγητές ιστού που χρησιμοποιούνται σήμερα είναι ο Internet Explorer της Microsoft και ο Firefox της Mozilla. Ο κάθε ένας από αυτούς τους περιηγητές αποθηκεύει, με την δική του μορφοποίηση, την δραστηριότητα περιήγησης στο διαδίκτυο των διαφόρων χρηστών που έχουν λογαριασμούς χρήστη σε ένα σύστημα. Ο Internet Explorer αποθηκεύει το ιστορικό περιήγησης ενός χρήστη σε ένα αρχείο με όνομα index.dat και ο Firefox αποθηκεύει την δραστηριότητα περιήγησης στο διαδίκτυο σε ένα αρχείο με όνομα history.dat. Αυτά τα δύο αρχεία είναι κρυφά αρχεία. Προκειμένου να τα δούμε ο περιηγητής ιστού θα πρέπει να έχει ρυθμιστεί ώστε να προβάλει τόσο τα κρυμμένα αρχεία όσο και τα αρχεία συστήματος. Αυτά τα δύο αρχεία δε μπορούν να σβηστούν με κάποιο συνηθισμένο τρόπο. Η δικανική διαδικτύου μεταχειρίζεται κρίσιμες πληροφορίες σχετικά με ένα έγκλημα ερευνώντας το ιστορικό περιήγησης ενός ατόμου, τον αριθμό των επισκέψεων του σε ένα ιστοτόπο, την διάρκεια κάθε επίσκεψης, τα αρχεία που κατέβασε και ανέβασε στο συγκεκριμένο ιστοτόπο, την ρύθμιση των cookies και άλλες κρίσιμες πληροφορίες. Θα παρουσιάσουμε με συντομία δύο σχετικά εργαλεία.

4.4.1 Mandriant Web Historian

Το εργαλείο αυτό βοηθά τους χρήστες να κάνουν επισκόπηση των URL των ιστοσελίδων που είναι αποθηκευμένες στα αρχεία ιστορικού περιήγησης για τους περισσότερο χρησιμοποιούμενους περιηγητές ιστού. Με με τη χρήση του εργαλείου αυτού ο διερευνητής δικτύων μπορεί να καθορίσει τι, πότε, που και πως είδε ο εισβολέας στις διάφορες ιστοσελίδες. Το εργαλείο Web Historian μπορεί να χρησιμοποιηθεί για την ανάλυση ενός συγκεκριμένου αρχείου ιστορικού περιήγησης ή μπορεί να αναζητήσει σε ένα δεδομένο φάκελο αρχείων ή δίσκο και να βρει όλα τα αρχεία ιστορικού περιήγησης. Το Web Historian παράγει μία αναφορά η οποία περιλαμβάνει την διαδικτυακή δραστηριότητα όλων των αρχείων ιστορικού περιήγησης που μπορεί να εντοπίσει.

4.4.2 Index.dat analyzer

Το Index.dat analyzer είναι ένα εργαλείο διερεύνησης που χρησιμεύει για την επισκόπηση, ανάλυση και διαγραφή των περιεχομένων των αρχείων index.dat. Το εργαλείο αυτό μπορεί να χρησιμοποιηθεί ώστε να παρακολουθηθεί το ιστορικό περιήγησης ιστού, τα cookies και η κρυφή μνήμη. Ακόμη το εργαλείο παρέχει τη δυνατότητα να ανοίγει το αρχείο που ανέβηκε ή κατέβηκε από την ιστοσελίδα. Τέλος το εργαλείο παρέχει πληροφορίες για τα cookies οι οποίες περιλαμβάνουν την ιστοσελίδα που συσχετίζεται με το cookie, την ημερομηνία και ώρα που δημιουργήθηκε για πρώτη φορά το cookie και άλλες σχετικές πληροφορίες. (Meghanathan, 2009).

5. Εργαστήριο Network Forensics

Σε αυτό το σημείο θα προταθεί ένα εργαστήριο Network Forensics το οποίο θα πρέπει να πληρεί κάποιες απαιτήσεις και προδιαγραφές εξοπλισμού. Παρακάτω θα παρουσιαστεί ένα διάγραμμα του εργαστηρίου και τέλος θα γίνουν κάποιες ρυθμίσεις.

5.1 Απαιτήσεις

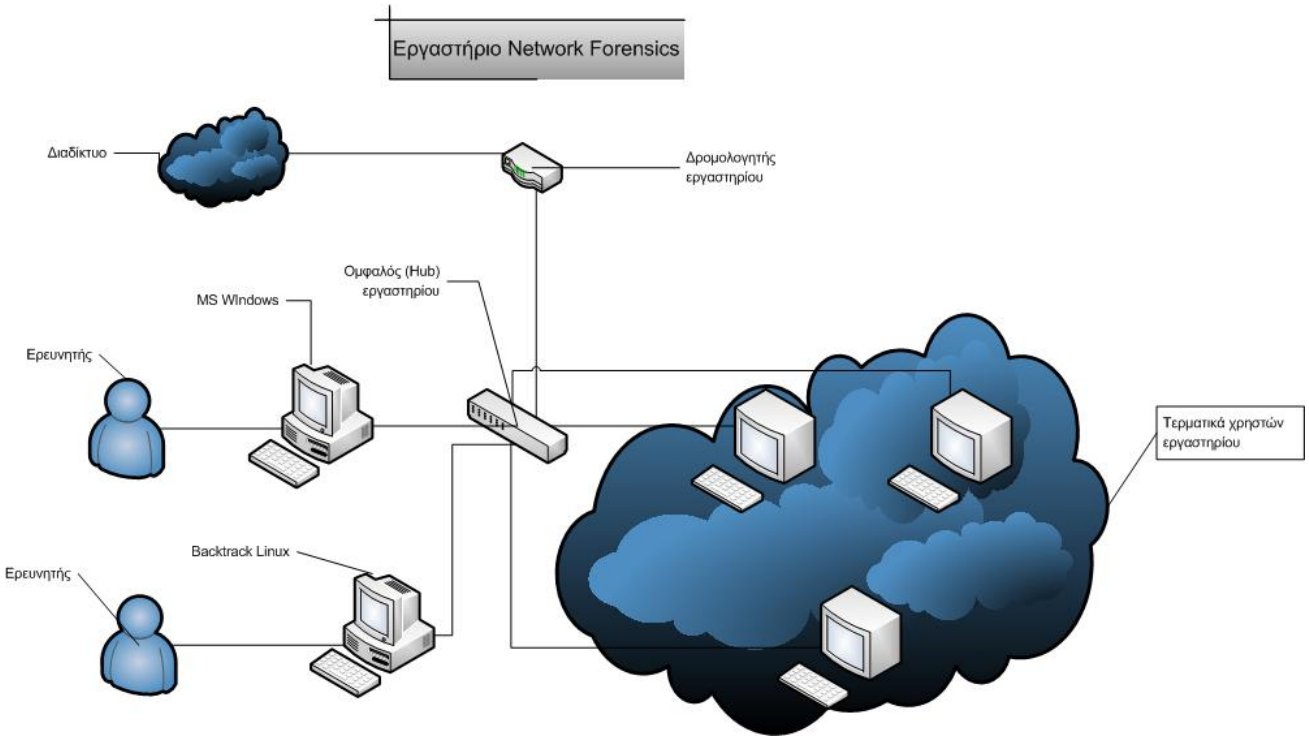
Σύμφωνα με τα γραφόμενα στα παραπάνω κεφάλαια, θα πρέπει να πληρούνται κάποιες απαιτήσεις στο εργαστήριο Network Forensics. Αναλυτικότερα:

1. Ο ερευνητής θα πρέπει να έχει είτε φυσική είτε απομακρυσμένη πρόσβαση στο σύστημα καθώς και πλήρη δικαιώματα χρήσης όλων των υποσυστημάτων του δικτύου ώστε να μπορεί να γίνει η διερεύνηση δικτύων.
2. Ο ερευνητής διενεργεί την έρευνα είτε την στιγμή που εξελίσσεται, για παράδειγμα μία επίθεση, είτε σε μεταγενέστερο χρονικό σημείο.

Για το συγκεκριμένο εργαστήριο θεωρούμε ότι ο ερευνητής έχει φυσική πρόσβαση στο δίκτυο όπου υπάρχει το σύστημα στόχος.

5.2 Χωροταξία

Για την δημιουργία του εργαστηρίου θα τοποθετηθούν ένας δρομολογητής ο οποίος συνδέει τα υπολογιστικά συστήματα του δικτύου με το διαδίκτυο. Με τη σειρά του ο δρομολογητής θα συνδεθεί με ένα ομφαλό (hub) είτε με ένα μεταγωγέα Cisco. Ακόμη τοποθετείται ένα σύστημα ανίχνευσης παρείσφρησης (IDS) στον ομφαλό. Επίσης τοποθετείται στο δίκτυο ένας υπολογιστής ο οποίος συνδέεται με τον ομφαλό και θα χρησιμοποιηθεί και αυτός για διερεύνηση στο δίκτυο. Χρησιμοποιώντας αυτά τα δύο συστήματα επιτυγχάνουμε καλύτερα αποτελέσματα ώστε να μη χαθεί κάποια πληροφορία που δεν έχει διερευνηθεί. Τέλος στον ομφαλό συνδέονται τρία ή και περισσότερα τερματικά συστήματα στα οποία θα γίνει η διερεύνηση δικτύου.



Εικόνα 13: Χάρτης εργαστηρίου network forensics

5.3 Εξοπλισμός

Όσον αφορά τον εξοπλισμό που θα χρησιμοποιηθεί εξαρτάται από τις απαιτήσεις του περιβάλλοντος. Εάν η κίνηση στο δίκτυο είναι υψηλή τότε θα χρησιμοποιηθεί ως σύστημα ανίχνευσης παρείσφρησης ένα υπολογιστικό σύστημα με υψηλές προδιαγραφές. Σε άλλη περίπτωση μπορεί να χρησιμοποιηθεί ως IDS ένα μέτριο υπολογιστικό σύστημα. Ακόμη για το δεύτερο υπολογιστικό σύστημα το οποίο συνδέεται με τη σειρά του με τον ομφαλό απαιτείται να είναι ισχυρό ανάλογα με τον αριθμό των πακέτων που περνούν από το δρομολογητή. Για το συγκεκριμένο εργαστήριο θα χρησιμοποιηθούν ισχυρά υπολογιστικά συστήματα διότι συγκεντρώνονται πολλές συνδέσεις στο δίκτυο. Κατά προτίμηση και στα δύο υπολογιστικά συστήματα τα οποία θα χρησιμοποιηθούν για διερεύνηση του εργαστηρίου απαιτούνται να έχουν επεξεργαστή τουλάχιστον δύο πυρήνων, μνήμη RAM 4GB καθώς και σκληρό δίσκο τουλάχιστον 1TB για την αποθήκευση των απαιτούμενων πληροφοριών που θα συλλεχθούν κατά τη διερεύνηση καθώς και μία κάρτα δικτύου. Τα τερματικά συστήματα του εργαστηρίου στα οποία συνδέονται οι τυπικοί χρήστες δεν χρειάζονται να απαιτούν συγκεκριμένες προδιαγραφές. Ως δρομολογητή του εργαστηρίου αρκούμαστε σε ένα

τυπικό δρομολογητή. Τέλος ως ομφαλός μπορεί να χρησιμοποιηθεί ένας τυπικός ομφαλός με τουλάχιστον οκτώ θύρες είτε ένας μεταγωγέας Cisco Catalyst 2900XL ώστε να εκμεταλλευτούμε την τεχνολογία SPAN και να μπορούμε να επιτύχουμε παρακολούθηση της κίνησης στο δίκτυο. Η χρήση του μεταγωγέα Cisco μπορεί να επιτύχει καλύτερα αποτελέσματα στη διαδικασία της διερεύνησης καθώς δεν θα έχουμε απώλεια πακέτων, γεγονός που μπορεί να προκύψει εάν χρησιμοποιήσουμε έναν ομφαλό.

5.4 Ρυθμίσεις

5.4.1 Ρυθμίσεις στα MS Windows

5.4.1.1 Ρυθμίσεις του Snort

Στο πρώτο υπολογιστικό σύστημα το οποίο λειτουργεί ως IDS χρησιμοποιούμε το λειτουργικό σύστημα MS Windows. Κατεβάζουμε το snort από την ιστοσελίδα http://www.snort.org. Το Snort έχει ως προαπαιτούμενο το λογισμικό WinPcap το οποίο κατεβάζουμε από την ιστοσελίδα http://www.winpcap.org. Εγκαθιστούμε και τα δύο πακέτα ακολουθώντας τις προεπιλεγμένες ρυθμίσεις. Στην συνέχεια ανοίγουμε το αρχείο snort.conf με κάποιον editor από την προεπιλεγμένη διαδρομή C:\Snort\etc. Στην γραμμή ipvar HOME_NET ορίζουμε το δίκτυο στο οποίο θα γίνει η διερεύνηση. Στη συνέχεια ορίζουμε τον DNS Server στη γραμμή ipvar DNS_SERVERS. Επίσης στις παρακάτω ρυθμίσεις ορίζουμε όλους τους web servers ή smtp servers ή sql servers κ.ο.κ ανάλογα με τις απαιτήσεις μας. Επίσης μπορούμε να αλλάξουμε τη διαδρομή του φακέλου όπου τοποθετούνται οι κανόνες του Snort στη γραμμή var RULE_PATH, προεπιλεγμένα είναι η διαδρομή C:\Snort\rules, στη γραμμή var SO_RULE_PATH, ορίζουμε το φάκελο c:\snort\so_rules (τον οποίο δημιουργούμε αν δεν υπάρχει) και στη γραμμή var PREPROC_RULE_PATH ορίζουμε το φάκελο c:\snort\preproc_rules. Στη συνέχεια στη γραμμή # path to dynamic preprocessor libraries αλλάζουμε στη διαδρομή C:\Snort\lib\snort_dynamicpreprocessor, στη γραμμή # path to base preprocessor engine, αλλάζουμε στη διαδρομή του αρχείου C:\Snort\lib\snort_dynamicengine\sf_engine.dll και

στη γραμμή # path to dynamic rules libraries αλλάζουμε στη διαδρομή C:\Snort\lib\snort_dynamicrules (τον οποίο δημιουργούμε αν δεν υπάρχει). Στη συνέχεια στη γραμμή # metadata reference data. do not modify these lines αλλάζουμε στις δύο εντολές include τις διαδρομές των αρχείων σε C:\Snort\etc\classification.config και C:\Snort\etc\reference.config αντίστοιχα. Ακόμη κάτω από τη γραμμή # output log_tcpdump: tcpdump.log τοποθετούμε την παρακάτω παράμετρο output alert_fast: alerts.ids. Στη συνέχεια στη διαδρομή C:\Snort\log δημιουργούμε ένα κενό αρχείο με όνομα alerts.ids. Στη συνέχεια δημιουργούμε ένα λογαριασμό στην ιστοσελίδα του Snort και κατεβάζουμε το συμπιεσμένο αρχείο με την τελευταία έκδοση των κανόνων. Αποσυμπιέζουμε το συμπιεσμένο αρχείο με κατάληξη tar στον φάκελο εγκατάστασης του Snort που προεπιλεγμένα είναι η διαδρομή C:\Snort\.

5.4.1.2 Ρυθμίσεις του Nmap

Στο πρώτο υπολογιστικό σύστημα εγκαθιστούμε επιπλέον την εφαρμογή Nmap. Κάνουμε λήψη της τελευταίας σταθερής έκδοσης από την ιστοσελίδα http://nmap.org/download.html. Εγκαθιστούμε το αρχείο εγκατάστασης με τις προεπιλεγμένες ρυθμίσεις από το πρόγραμμα.

5.4.1.3 Ρυθμίσεις του Wireshark

Στο πρώτο υπολογιστικό σύστημα εγκαθιστούμε επιπλέον την εφαρμογή Wireshark. Κάνουμε λήψη της τελευταίας σταθερής έκδοσης από την ιστοσελίδα http://www.wireshark.org/download.html. Εγκαθιστούμε το αρχείο εγκατάστασης με τις προεπιλεγμένες ρυθμίσεις από το πρόγραμμα.

5.4.2 Ρυθμίσεις στο Backtrack Linux

Στο δεύτερο υπολογιστικό σύστημα δε χρειάζεται να προβούμε σε εγκατάσταση των p0f και xrobe2 μιας και είναι προεγκατεστημένα στο λειτουργικό σύστημα Backtrack.

5.4.2.1 Ρυθμίσεις του Pyflag

Το Pyflag έχει κάποιες προαπαιτούμενες εφαρμογές. Τα εγκαθιστούμε διαδοχικά με τις παρακάτω εντολές στο τερματικό: apt-get install python-dev (python dev files), apt-get install python-mysqldb (MySQLdb), apt-get install python-dateutil (dateutil), apt-get install python-urwid (urwid), apt-get install libewf-dev (libewf for EWF image support),), apt-get install clamav-daemon (clamd for Virus Scanning Support). Τέλος εγκαθιστούμε το πακέτο clamav-data για να αποθηκευθούν οι υπογραφές του clamd. Η εγκατάσταση γίνεται με την εντολή apt-get install clamav-data. Στη συνέχεια για να είναι ρυθμισμένη σωστά η MySQL ώστε να γνωρίζει τη σωστή ζώνη ώρας, εκτελούμε την παρακάτω εντολή στο τερματικό: mysql_tzinfo_to_sql usr/share/zoneinfo/ | mysql –uroot –p mysql. Στη συνέχεια γίνεται εγκατάσταση του darcs για να μπορεί στη συνέχεια να γίνει λήψη της τελευταίας έκδοσης του pyflag. Εκτελούμε την παρακάτω εντολή στο τερματικό: apt-get install darcs automake autoconf libtool. Κατεβάζουμε την τελευταία έκδοση του πηγαίου κώδικα με την εντολή: darcs get http://www.pyflag.net/pyflag/. Μεταβαίνουμε στο φάκελο όπου κατέβηκε ο πηγαίος κώδικας με την εντολή: cd pyflag. Στη συνέχεια μεταγλωτίζουμε τον πηγαίο κώδικα με την παρακάτω εντολή: sh autogen.sh. Τέλος εκτελούμε στο τερματικό διαδοχικά τις εντολές ./configure, make, make install. Στη συνέχεια εκτελούμε στο τερματικό την εντολή pyflag. Μεταβαίνουμε στον Mozilla Firefox και μεταβαίνουμε στη διεύθυνση http://127.0.0.1:8000. Θα εμφανιστούν οι ρυθμίσεις του Pyflag όπου θα πρέπει να θέσουμε το συνθηματικό του χρήστη dbuser.

Στη συνέχεια εγκαθιστούμε την υπηρεσία GeoIP ώστε να μπορέσουμε να δούμε την τοποθεσία των απομακρυσμένων IP. Εκτελούμε τις παρακάτω εντολές διαδοχικά:

```
wget http://www.maxmind.com/download/geoip/api/c/GeoIP.tar.gz
tar -xvzf GeoIP.tar.gz
cd GeoIP*
./configure
make
sudo make install
```

Στη συνέχεια εγκαθιστούμε την εφαρμογή του GeoIP για Python:

wget http://www.maxmind.com/download/geoip/api/python/GeoIP-Python-1.2.1.tar.gz

tar -xvzf GeoIP-Python-1.2.1.tar.gz

cd GeoIP-Python*

sudo python setup.py install

Στη συνέχεια κατεβάζουμε και τοποθετούμε την βάση δεδομένων σε μία διαδρομή της προτίμησής μας:

wget http://www.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz

gunzip GeoLiteCity.dat.gz

mv GeoLiteCity.dat /usr/local/share/GeoIP

Στη συνέχεια ενημερώνουμε τη βάση δεδομένων του GeoIP που κατεβάσαμε προηγουμένως με το PyFlag:

PYFLAG_GEOIPDB=/usr/local/share/pyflag/GeoLiteCity.dat

5.4.2.2 Ρυθμίσεις του xplico

Το xplico είναι προεγκατεστημένο στο Backtrack Linux. Χρειάζεται να εγκατασταθούν κάποια πακέτα τα οποία δεν έρχονται προεγκατεστημένα με το Backtrack Linux. Τα εγκαθιστούμε με την παρακάτω εντολή:

apt-get install libnet1-dev librecode0 libxaw7-dev libxext-dev libxmu-dev libxmu-headers libxpm-dev python3-all recode x11proto-xext-dev.

Για να λειτουργήσει σωστά χρειάζεται να γίνει εγκατάσταση του πακέτου GeoIP. Το εγκαθιστούμε στην τελευταία έκδοση εκτελώντας τις παρακάτω εντολές στο τερματικό:

```
wget http://geolite.maxmind.com/download/geoip/api/c/GeoIP-1.4.8.tar.gz
tar zxvf GeoIP-1.4.8.tar.gz
cd GeoIP-1.4.8
./configure
make
cd ..
rm -f *.tar.gz
```

Στη συνέχεια θα εγκαταστήσουμε το πακέτο videosnarf εκτελώντας τις παρακάτω εντολές στο τερματικό:

```
wget http://downloads.sourceforge.net/project/ucsniff/videosnarf/videosnarf-0.63.tar.gz
tar xvzf videosnarf-0.63.tar.gz
cd videosnarf-0.63
./configure
make
cd ..
cp videosnarf-0.63/src/videosnarf xplico-0.6.3
```

Στη συνέχεια πλοηγούμαστε στο αρχείο /etc/apache2/ports.conf όπου βλέπουμε ότι έχει ήδη προστεθεί μία γραμμή Listen 9876 η οποία είναι η προεπιλεγμένη θύρα όπου λειτουργεί το xplico. Προσθέτουμε πριν από αυτήν τη γραμμή τα παρακάτω:

```
# xplico Host port
NameVirtualHost *:9876
```

Στη συνέχεια πλοηγούμαστε στο αρχείο /etc/php5/apache2/php.ini. Σε αυτό το αρχείο αλλάζουμε τις τιμές των post_max_size και upload_max_filesize σε 100M.

6. Σενάρια – Ασκήσεις

6.1 Snort

Εργαστηριακή Άσκηση για το εργαλείο

Snort

6.1.1 Γενικά για το εργαλείο Snort

Το Snort είναι ένα απλό εργαλείο γραμμής εντολών το οποίο χρησιμοποιείται για την παρακολούθηση της κίνησης δικτύου, αναζητώντας για υπογραφές παραβίασης βάσει κανόνων, εκτυπώνοντας ειδοποιήσεις στη οθόνη και δημιουργώντας αρχείο καταγραφής όταν γίνει αντιστοίχηση ενός κανόνα, εκτελώντας ανάλυση πρωτοκόλλων, επιδιορθώνοντας το δίκτυο, και ελέγχοντας τις μη εξουσιοδοτημένες εφαρμογές. Το Snort μπορεί να παρακολουθήσει όλη την δικτυακή κίνηση σε έναν υπολογιστή ή μπορεί να τοποθετηθεί σε ένα προσαρμογέα δικτύου ώστε να παρακολουθήσει όλη την κίνηση πάνω στην διασύνδεση. Στην άσκησή μας θα επικεντρωθούμε στη χρήση του Snort ως εργαλείο ανίχνευσης εισβολών, θα εξοικειωθούμε με τις εντολές, τις επιλογές που μας παρέχει, θα μάθουμε να αναγνωρίζουμε τις ειδοποιήσεις που μας εμφανίζει και θα δημιουργήσουμε ένα κανόνα ο οποίος θα μας ειδοποιεί όταν εκτελεστεί μία συγκεκριμένη ενέργεια.

6.1.2 Άσκηση

Μεταβαίνουμε στο υπολογιστικό σύστημα του ερευνητή το οποίο εκτελεί MS Windows και απαντούμε τις παρακάτω ερωτήσεις:

1. Εκτελέστε το command prompt των Windows. Μεταβείτε στη διαδρομή του εκτελέσιμου

αρχείου Snort. Εκτελέστε την εντολή snort –W. Τι παρατηρείτε;

Απάντηση: Το Snort εμφανίζει τις διαθέσιμες διεπαφές δικτύου στο υπολογιστικό σύστημα.

Η παράμετρος W απαριθμεί τις διαθέσιμες διεπαφές δικτύου.

2. Εκτελέστε την εντολή snort –v –iX (όπου X ο αριθμός της διεπαφής). Τι παρατηρείτε;

   Απάντηση: Το Snort κάνει sniffing την επιλεγμένη διεπαφή δικτύου εκτυπώνοντας στην οθόνη όλα τα πακέτα.

   v verbose, i interface

3. Εκτελέστε την εντολή snort -iX -s -l c:\snort\log\ -c c:\snort\etc\snort.conf –T (όπου X ο αριθμός της διεπαφής). Τι παρατηρείτε;

   Απάντηση: Το Snort επαλήθευσε τις ρυθμίσεις σε αυτή τη διεπαφή δικτύου.

   Η παράμετρος s δημιουργεί ειδοποιήσεις στο αρχείο καταγραφής. Η παράμετρος l δημιουργεί φάκελο με όνομα την IP του απομακρυσμένου μηχανήματος για το οποίο δημιουργήθηκε η ειδοποίηση. Με την παράμετρο c χρησιμοποιείται το αρχείο καταγραφής. Με την παράμετρο T το Snort κάνει διαγνωστικό έλεγχο ότι όλα λειτουργούν σωστά.

4. Εκτελέστε την εντολή snort –vd. Τι παρατηρείτε;

   Απάντηση: Αυτή η εντολή επιστρέφει τις κεφαλίδες TCP/IP και λεπτομερείς πληροφορίες των πακέτων.

5. Εκτελέστε την εντολή snort –A console -iX –c C:\Snort\etc\snort.conf –l c:\Snort\log –K ascii (όπου X ο αριθμός της διεπαφής). Τι παρατηρείτε;

   Απάντηση: Το Snort λειτουργεί ως sniffer αποθηκεύοντας στο log file όλες τις ειδοποιήσεις που ταιριάζουν με τους κανόνες που εισαγάγαμε στο Snort.

   Η παράμετρος –A console εκτυπώνει τις ειδοποιήσεις στην κονσόλα. Η παράμετρος –K ascii χρησιμοποιείται για να αποθηκεύσει το αρχείο καταγραφής σε μορφοποίηση χαρακτήρων ASCII.

6. Ορίστε ένα κανόνα ο οποίος δημιουργεί ειδοποίηση στο Snort ότι συνδέθηκε ένας χρήστης στο facebook.

   Απάντηση: alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "USER CONNECTED TO FACEBOOK"; content:"GET"; content:"facebook"; sid: 1100026; rev:1;)

6.2 Pyflag

Εργαστηριακή Άσκηση για το εργαλείο

Pyflag

6.2.1 Γενικά για το εργαλείο Pyflag

Το εργαλείο PyFlag είναι ένα ανεπτυγμένο εργαλείο ανάλυσης αρχείων καταγραφής μεγάλο όγκου όπως αντίγραφα σκληρών δίσκων και αρχεία καταγραφών δικτύου. Το PyFlag είναι ικανό να αναλύσει αρχεία καταγραφής δικτύου μορφοποίησης του tcpdump και υποστηρίζει μεγάλο αριθμό δικτυακών πρωτοκόλλων. Είναι ικανό να εξάγει πληροφορίες υψηλού επιπέδου και να εντοπίσει με ακρίβεια από πού εξάχθηκε κάθε κομμάτι δεδομένων. Τα βασικά συστατικά του εργαλείου αυτού είναι η αναδημιουργία ροής, ο χειριστής πακέτων και η διχοτόμηση των ροών δεδομένων. Το PyFlag δέχεται ως εισαγωγή αρχεία pcap, εξάγει τα πακέτα και τα διχοτομεί σε χαμηλότερα επίπεδα πρωτοκόλλων (IP, TCP ή UDP). Τα συσχετιζόμενα πακέτα συλλέγονται σε ροές χρησιμοποιώντας την αναδημιουργία ροής. Αυτές οι ροές στη συνέχεια διχοτομούνται σε υψηλότερα επίπεδα πρωτοκόλλων (HTTP, IRC και άλλα). Το PyFlag αναδημιουργεί συνόδους HTTP και είναι ικανό να διχοτομήσει εφαρμογές υψηλού επιπέδου όπως εφαρμογές ηλεκτρονικού ταχυδρομείου. Αναγνωρίζει τους τύπους των αρχείων και παρουσιάζει το εικονικό σύστημα αρχείων σε μορφή δέντρου. Επίσης παρουσιάζεται η κίνηση μεταξύ διαφόρων πηγών και προορισμών και προς τις δύο κατευθύνσεις. Επίσης γίνεται επισκόπηση των περιεχομένων κάθε πακέτου και πρωτοκόλλου.

6.2.2 Άσκηση

Μεταβαίνουμε στο υπολογιστικό σύστημα του ερευνητή το οποίο εκτελεί το Backtrack Linux, εκκινούμε το Wireshark ή το tcpdump και καταγράφουμε την κίνηση στη διεπαφή δικτύου που μας ενδιαφέρει. Ανοίγουμε τον Mozilla Firefox και πλοηγούμαστε στο google.com, στο gmail όπου ανοίγουμε ένα εισερχόμενο email και σε μία ακόμη ιστοσελίδα της προτίμησής μας. Πως μπορούμε

να ανακτήσουμε τη δικτυακή κίνηση και να οπτικοποιήσουμε το ιστορικό του Mozilla Firefox με τη χρήση του PyFlag;

Απάντηση: Διακόπτουμε την καταγραφή της κίνησης με το Wireshark, και αποθηκεύουμε την καταγεγραμμένη κίνηση ως αρχείο pcap στο φάκελο /tmp/. (Εάν χρησιμοποιήσουμε το tcpdump εκτελούμε την παρακάτω εντολή στο τερματικό :tcpdump –w <όνομα_αρχείου>.pcap –i <διεπαφή_δικτύου>). Μεταβαίνουμε στη διεύθυνση http://127.0.0.1:8000. Δημιουργούμε μία νέα υπόθεση επιλέγοντας Case Management. Θέτουμε ένα όνομα για της υπόθεση, για παράδειγμα testcase, και κάνουμε submit. Επιλέγουμε από το μενού Load Data και την επιλογή Load IO Data Source. Επιλέγουμε στο Select IO Subsystem την επιλογή Standard. Στην επιλογή Select Standard image γράφουμε / και το όνομα του αρχείου που καταγράψαμε προηγουμένως με το wireshark. Πληκτρολογούμε στο Enter partition offset μία αριθμητική τιμή, και στο Unique Data Load ID μία τιμή για παράδειγμα PCAP. Στο επόμενο μενού που εμφανίζεται βλέπουμε ότι αυτόματα αναγνωρίστηκε το αρχείο που εισαγάγαμε ως αρχείο Pcap επιλέγουμε ως VFS Mount Point το χαρακτήρα /. Στη συνέχεια βλέπουμε ότι το PyFlag ανέλυσε τις ροές δεδομένων. Στη συνέχεια επιλέγοντας το πλήκτρο Home μπορούμε να δούμε την ανάλυση που έκανε το PyFlag. Από αυτό το μενού μπορούμε να δούμε τις συνδέσεις που εγκαθιδρύθηκαν, επιλέγοντας View Connections, όπου γίνεται ανάλυση τόσο της IP προορισμού και προέλευσης, τη θύρα επικοινωνίας και το χρόνο που έγινε η σύνδεση. Ανοίγοντας το Inode που επιθυμούμε μπορούμε να δούμε στην επιλογή Combined Stream το σύνολο της συνεδρίας. Ακόμη το PyFlag μας εμφανίζει κάποια διαθέσιμα Web Applications όπως το Webmail, τις αναζητήσεις στο Google (όπου μπορούμε να δούμε τις αναζητήσεις Google που ανακτήθηκαν) καθώς και τα HTML URL όπου και πάλι μπορούμε να δούμε τις ιστοσελίδες όπως αυτές ανακτήθηκαν. Ακόμη αν πλοηγηθούμε στις καρτέλες Communications, Web, Domains όπου βλέπουμε όλα τα domains που επισκεφθήκαμε.

6.3 P0f

6.3.1 Γενικά για το εργαλείο P0f

Το p0f είναι ένα ευέλικτο παθητικό εργαλείων ανίχνευσης λειτουργικών συστημάτων. Το p0f μπορεί να ανιχνεύσει μηχανήματα τα οποία συνδέονται με το σύστημα στόχο, συστήματα στα οποία συνδέεται το σύστημα στόχος, και συσκευές οι οποίες βρίσκονται πίσω από ένα πακέτο που λήφθηκε. Ακόμη μπορεί να εντοπίσει το φυσικό μέσο με το οποίο είναι συνδεδεμένο το απομακρυσμένο σύστημα, την απόσταση στην οποία βρίσκεται και το χρόνο που είναι σε λειτουργία. Το p0f εντοπίζεται το απομακρυσμένο σύστημα εξετάζοντας διάφορα πεδία στην διεύθυνση IP και τις κεφαλίδες TCP του TCP SYN ή τα πακέτα SYN/ACK τα οποία προέρχονται από το απομακρυσμένο σύστημα.

6.3.2 Άσκηση

Εκτελέστε την εντολή p0f -i ethX –vto <όνομα αρχείο>.txt (όπου X ο αριθμός της διεπαφής δικτύου). Τι παρατηρείτε;

Απάντηση: Αυτή η εντολή καταγράφει στο αρχείο που θέσαμε όλα τα συστήματα, με το όνομα του λειτουργικού συστήματος που εκτελούν, την IP τους, την ώρα της καταγραφής, την απόστασή τους από τη διεπαφή δικτύου, και τη δικτυακή σύνδεση.

Η παράμετρος -i επιτρέπει την επιλογή της συσκευής από την οποίο το p0f θα εξάγει τα πακέτα. Η παράμετρος –v υποδεικνύει ότι το p0f λειτουργεί ως verbose, η παράμετρος –t προσθέτει την ώρα της καταγραφής και η παράμετρος –o δείχνει στο αρχείο όπου γίνεται η καταγραφή.

6.4 Xprobe2

6.4.1 Γενικά για το εργαλείο Xprobe2

Το Xprobe2 είναι ένα δυναμικό εργαλείο απομακρυσμένης αναζήτησης ιχνών σε λειτουργικά συστήματα. Το Xprobe2 περιλαμβάνει ένα εργαλείο ανίχνευσης TCP, ένα ανιχνευτή θυρών, αυτόματο έλεγχο λήξης χρόνου για τα διάφορα εργαλεία του, δυνατότητα πλήρη ελέγχου όλων των λειτουργιών του και μία βάση δεδομένων υπογραφών με πάνω από 160 υπογραφές. Το Xprobe2 λειτουργεί εφαρμόζοντας στατιστική ανάλυση βασισμένη σε ένα μαθηματικό αλγόριθμο παρέχοντας το καλύτερο δυνατό ταίριασμα μεταξύ των δεδομένων που λήφθηκαν από το σύστημα στόχο και τη βάση δεδομένων υπογραφών.

6.4.2 Άσκηση

Εκκινήστε το εργαλείο Xprobe2 στο Backtrack Linux και χρησιμοποιώντας το εργαλείο αυτό εκτελέστε μία αναζήτηση σε ένα σύστημα στόχο και ελέγξτε την κατάσταση των θυρών TCP 20-40 και 80 και των θυρών UDP 500-540. Καταγράψτε τις παρατηρήσεις σας.

Απάντηση: Η εντολή που εκτελούμε στο τερματικό είναι η εξής: xprobe2 –v –U 500-540 –T 20-40,80 XXX.XXX.XXX.XXX (όπου XXX.XXX.XXX.XXX η καθορισμένη IP). Το Xprobe2 μας παρουσιάζει τα στατιστικά των θυρών TCP και UDP, δηλαδή πόσες από αυτές τις θύρες είναι ανοικτές, κλειστές ποιες είναι φιλτραρισμένες αλλά και ποιες υπηρεσίες εκτελούνται στις συγκεκριμένες θύρες. Τέλος το xprobe μας παρουσιάζει βάση πιθανοτήτας το εκτελούμενο λειτουργικό σύστημα στον υπολογιστή στόχο.

Η παράμετρος –v υποδεικνύει ότι το xprobe2 λειτουργεί ως verbose, η παράμετρος –U υποδεικνύει τις θύρες UDP που αναγνωρίζονται και η παράμετρος –T υποδεικνύει τις θύρες TCP που αναγνωρίζονται.

6.5 Xplico

6.5.1 Γενικά για το εργαλείο Xplico

Το xplico είναι ένα εργαλείο ανάλυσης της δικανικής δικτύων. Η κύρια εργασία του Xplico είναι η εξαγωγή δεδομένων από μία καταγραφή δικτύου (είτε ένα από ένα αρχείο .pcap είτε κάνοντας καταγραφή σε πραγματικό χρόνο).

6.5.2 Άσκηση

Εκκινήστε το εργαλείο xplico στο Backtrack Linux μεταβαίνοντας στη διαδρομή των μενού Applications > Backtrack > Forensics > Network Forensics > xplico web gui και δημιουργήστε μία νέα καταγραφή με αυτό το εργαλείο. Τι συμπεράσματα εξάγετε;

Απάντηση: Μεταβαίνουμε στο Mozilla Firefox και πλοηγούμαστε στη διεύθυνση http://127.0.0.1:9876. Στη φόρμα εισόδου θέτουμε ως όνομα χρήστη και συνθηματικό χρήστη το xplico (είναι τα προεπιλεγμένα στοιχεία εισόδου για το xplico). Στη συνέχεια δημιουργούμε μία νέα υπόθεση case επιλέγοντας New Case και στη συνέχεια επιλέγουμε Live acquisition και θέτουμε ένα όνομα για την υπόθεση. Στη συνέχεια επιλέγουμε την υπόθεση που μόλις δημιουργήσαμε και δημιουργούμε μία νέα συνεδρία και επιλέγουμε New Session. Δίνουμε ένα όνομα στη συνεδρία μας και την επιλέγουμε ώστε να δούμε περισσότερες πληροφορίες. Από την ιστοσελίδα που εμφανίζεται επιλέγουμε μία δικτυακή διεπαφή και εκκινούμε την καταγραφή. Μπορούμε να δούμε σε πραγματικό χρόνο την αποκωδικοποίηση των πακέτων. Μεταβαίνοντας στο μενού Graphs DNS μπορούμε να κάνουμε επισκόπηση των πραγματικών ονομάτων των DNS, να εκτελέσουμε αναζήτηση, αλλά και να δούμε ένα γράφημα με τις αποκρίσεις των DNS με βάση τον χρόνο, και ένα δεύτερο γράφημα με τον αριθμό των αποκρίσεων DNS με βάση το πραγματικό όνομα των DNS. Μεταβαίνοντας στην καρτέλα Arp μπορούμε να δούμε τις IP και τα ονόματα MAC των συστημάτων από τα οποία δημιουργούνται συνδέσεις. Από το μενού Web και Site μπορούμε όλες τις πληροφορίες

υψηλού επιπέδου που ανέκτησε το xplico στο Web. Μπορούμε να δούμε τις ιστοσελίδες στις οποίες έγινε επίσκεψη, τις εικόνες, βίντεο, ήχο και αρχεία flash που ανακτήθηκαν. Ακόμη από τα μενού Feed και Images βλέπουμε αντίστοιχα τα feeds και τις εικόνες που ανακτήθηκαν. Ακόμη μπορούμε να δούμε όλα τα MMS, τα μηνύματα ηλεκτρονικού ταχυδρομείου, όλα τα αρχεία που κατέβηκαν είτε από HTTP είτε FTP, όλες τις συνομιλίες μέσω Facebook, IRC, Paltalk και MSN αλλά και τιςς συνόδους μέσω VoIP. Τέλος για τα πακέτα που δεν αποκωδικοποιήθηκαν έχουμε τη δυνατότητα να αποθηκεύσουμε τα αρχεία pcap ώστε να εξάγουμε πληροφορίες με τη βοήθεια κάποιου άλλου εργαλείου. Το xplico αποθηκεύει στο φάκελο gea αρχεία kml τα οποία ανοίγουμε στο λογισμικό Google Earth και μπορούμε να δούμε με γραφικό τρόπο την γεωγραφική τοποθεσία των απομακρυσμένων υπολογιστών συστημάτων με τα πραγματικά ονόματά τους.

7. Συμπεράσματα

Μετά από εκτενή μελέτη του κλάδου της επιστήμης της δικανικής δικτύων σε βιβλιογραφικό επίπεδο, οδηγούμε στο συμπέρασμα ότι δεν υπάρχει σύμπλευση των ιδεών των συγγραφέων ως προς τη μεθοδολογία που χρησιμοποιείται στη δικανική δικτύων. Βέβαια ο Pilli λαμβάνοντας υπόψη όλες τις προγενέστερες μεθοδολογίες διερεύνησης δικτύων προτείνει ένα γενικό πλαίσιο το οποίο περιλαμβάνει όλες τις απαιτούμενες ενέργειες που πρέπει να επιτελεστούν στη διερεύνηση δικτύων και δίνει ώθηση προς την σωστή κατεύθυνση. Όσον αφορά τα εργαλεία που χρησιμοποιούνται στη διερεύνηση δικτύων, στις περισσότερες περιπτώσεις ο αναλυτής απαιτείται να χρησιμοποιήσει διαφορετικά εργαλεία για να καταλήξει σε ασφαλή συμπεράσματα, καθώς κάποια από τα εργαλεία όπως το Wireshark δε μπορεί να διαχειριστεί μεγάλο όγκο δεδομένων, και κάποια ολοκληρωμένα εργαλεία όπως το PyFlag δεν μπορεί να διχοτομήσει μεγάλο αριθμό πρωτοκόλλων σε σχέση με το Wireshark. Από την βιβλιογραφική επισκόπηση διαφαίνεται το γεγονός ότι υπάρχει θετική εξέλιξη ως προς τα διαθέσιμα εργαλεία που έχει στη διάθεσή του ο ερευνητής, καθώς τα τελευταία χρόνια έχουν κατασκευαστεί εξειδικευμένα μηχανήματα τα οποία διαχειρίζονται μεγάλο όγκο δεδομένων, διχοτομούν μεγάλο αριθμό πρωτοκόλλων και ελέγχουν για ύποπτες δραστηριότητες. Η υλοποίηση του εργαστηρίου των Network Forensics μας οδηγεί στο συμπέρασμα ότι ανακύπτει το γεγονός ότι λόγω του μεγάλου όγκου των δεδομένων που διακινούνται στο χώρο ενός οργανισμού υπάρχει σημαντική πιθανότητα είτε να χαθούν πακέτα από την διερεύνηση είτε να μειωθεί το διαθέσιμο εύρος ζώνης στους χρήστες του οργανισμού. Η λύση που προτείνεται σε αυτό το ζήτημα είναι η προσεκτική μελέτη του δικτύου του οργανισμού ώστε να επιλεχθεί ο κατάλληλος εξοπλισμός για τη διερεύνηση του δικτύου του.

8. Βιβλιογραφία

1. Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition ,Academic Press , 2004.

2. Vanzant, D., FBI CART, Law Enforcement Information Management Conference, http://www.nlectc.org/nlectcse/download/vanzant_may2002_leim.pdf.

3, Vais, M., ‘‘Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment Report,’’ Institute for Security Technology Studies, Dartmouth College, NH, June 2002.

4. Mohay, G. et al, Computer And Intrusion Forensics, Artech House, 2003.

5. A Road Map for Digital Forensic Research http://www.dfrws.org/2001/dfrws-rm-final.pdf

6. Caloyannides, M., Privacy Protection and Computer Forensics, Second Edition. Artech House, 2004

7. Kanellis, P. Et al, Digital Crime and Forensic Science in Cyberspace. Idea Group Inc., 2006.

8. Kent, K., Chevalier, S., Grance, T., & Dang, H., Guide to integrating forensic techniques into incident response: recommendations of the National Institute of Standards and Technology. NIST Special Publication, 800-86, 2006 http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

9. Garrlson C., Digital Forensics for Network, Internet, and Cloud Computing A Forensic Evidence Guide for Moving Targets and Data. Syngress, 2010.

10. Vacca J., Computer Forensics: Computer Crime Scene Investigation Second Edition. Charles River Media, 2005.

11. Brown C., Computer Evidence: Collection & Preservation. Charles River Media, 2006.

12. Li C. - T., Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions. Information Science Reference, 2010.

13. Meghanathan N., Allam S.R., & Moore L., International Journal of Network Security & Its Applications, Vol.1, No.1,April 2009.

14. http://www.forensicscience.org

15. Jansen W., Ayers R., Guidelines on Cell Phone Forensics, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-101, May 2007

16. Bell S., Encyclopedia of Forensic Science, Revised Edition, Infobase Publishing, 2008

17. Call for Cell Phone Forensics, National Law Enforcement and Corrections Technology Center System, TechBeat, Winter 2008

18. Pilli E., Joshi R.C., Niyogi R., A Generic Framework for Network Forensics, International Journal of Computer Application (0975 – 8887) Vol. 1 – No. 11, 2010

19. Arkin O., The Use of Xprobe2 in a Corporate Enviroment, Sys-Security Group, 2003

20. http://tools.netsa.cert.org/silk/

21. Orebaugh A., Pinkard B., Nmap In the Enterprise Your Guide to Network Scanning, Syngress, 2008

22. Casey E., Handbook of Computer Crime Investigation Forensics Tools and Technology, Academic Press, 2003

23. Paxson V., Bro: A System for Detecting Network Intruders in Real-Time, 7th USENIX Security Symposium, Jan. 1998.

24. Sira R., Network Forensics Analysis Tools: An Overview of an Emerging Texhnology, Sans Institute, 2003

25. Promise C., Mandia K. Incident Response & Computer Forensics, Second Edition, McGraw-Hill, 2003

26. Tullock M., Microsoft Encyclopedia of Security, Microsoft Press, 2003

27. http://www.netwitness.com/

28. http://lcamtuf.coredump.cx/p0f.shtml

29. Schweitzer D., Incident Response: Computer Forensics Toolkit, Wiley Publishing, Inc., 2003

30. http://ettercap.sourceforge.net/index.php

31. http://www.bro-ids.org/wiki/index.php/Main_Page

32.http://www.xplico.org