ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

CERTCOOP

ΤΕΧΝΙΚΟ ΕΓΧΕΙΡΙΔΙΟ

ΣΥΛΛΟΓΗ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ ΣΕ LINUX ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

./.

14.	Συμπεράσματα	
ΚΕΦΑΛΑΙΟ «Ε» ΣΥΓΚΕΝΤΡΩΣΗ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ		
15.	Ζητήματα/Εξετάσεις/Σκέψεις πριν την Συλλογή	
16.	Τα Βασικά για την Ψηφιακή Εγκληματολογική Ανάλυση σε Ένα Σύστημα Linux	
17.	Έναρξη της Διαδικασίας	
18.	Ανάκτηση Πτητικών - Προσωρινής Αποθήκευσης Πληροφοριών (Volatile Information)	
	Ανάκτηση Αντιγράφου Φυσικής Μνήμης (Physical Memory)	
	Καταγραφή Λεπτομερειών Συστήματος	
	Συνδεδεμένοι Χρήστες στο Σύστημα	
	Συνδέσεις και Δραστηριότητα Δικτύου	
	Τρέχουσες Διεργασίες	
	Συσχέτιση Θυρών και Διεργασιών	
	Εντοπισμός Ύποπτων Υπηρεσιών	
	Ανάκτηση Ενοτήτων Πυρήνα (Kernel Modules)	
	Εντοπισμός ανοικτών αρχείων	
	Ανάκτηση Ιστορικού Εντολών	
	Επιθεώρηση Κοινοχρήστων Δικτύου (Network Shares)	
	Εξέταση Προγραμματισμένων Εργασιών	
	Εξέταση Περιεχομένων Πρόχειρου (Clipboard)	
	Εντοπισμός των αρχείων setuid και setgid	
19.	Προσωρινά Αποθηκευμένες Πληροφορίες σε Προγράμματα Περιήγησης (διευθύνσεις, λήψη ιστορικού)	
	Συλλογή πληροφοριών από φυλλομετρητές	
	Ιστορικό αναζήτησης στο Διαδίκτυο	
	Τελευταίες αναζητήσεις	
	Cookies	
20.	Συλλογή Στατικών – Αποθηκευμένων Πληροφοριών (Non Volatile Information)	
	Ψηφιακά Σημασμένη Αναπαραγωγή των Μέσων Αποθήκευσης	
	Εξέταση Ρυθμίσεων Ασφαλείας Συστήματος	
	Σχέσεις των Έμπιστων Hosts	
	Εντοπισμός Μηχανισμών Επιμονής (Persistence	

ΚΕΦΑΛΑΙΟ «Α»

ΕΙΣΑΓΩΓΗ

ΤΜΗΜΑ 1
ΣΧΕΤΙΚΑ ΜΕ ΤΟΝ ΟΔΗΓΟ

Αυτός ο οδηγός παρέχει πληροφορίες σχετικά με την ψηφιακή εγκληματολογική ανάλυση ενός Linux λειτουργικού συστήματος. Επικεντρώνεται στη διαδικασία συγκέντρωσης αποδεικτικών στοιχείων και αναφέρεται στην έκδοση 16.04 LTS του Ubuntu. Τα παραδείγματα που αναφέρονται ισχύουν, σε πολλές περιπτώσεις και για τις παλαιότερες εκδόσεις του λειτουργικού, καθώς έχει παρόμοια δομή.

Παρέχει μια γενική παρουσίαση της διαδικασίας συλλογής αποδεικτικών στοιχείων, εξηγώντας από τι συνίσταται, για πιο λόγο πραγματοποιείται, τα στάδια που την απαρτίζουν, τις μεθόδους για να την πραγματοποιήσουμε και ταυτόχρονα δίνει μία συγκεκριμένη μεθοδολογία. Ο οδηγός παρουσιάζει μία γενική εικόνα της ψηφιακής εγκληματολογικής ανάλυσης και εστιάζει κυρίως στη φάση της απόκτησης-συλλογής των αποδεικτικών στοιχείων και αυτή είναι η βασική επιδίωξη του.

Το κοινό-στόχος αυτού του εγγράφου είναι οι επαγγελματίες του τομέα της πληροφορικής (τεχνικοί υποστήριξης, διαχειριστές συστήματος, διαχειριστές δικτύου, αναλυτές ιομορφικού λογισμικού, κ.λπ.) που έχουν γνώση των υπολογιστών, αλλά δεν είναι εξοικειωμένοι με την ψηφιακή διαδικασία εγκληματολογικής ανάλυσης και μπορεί να χρειαστεί να αντιμετωπίσουν ένα περιστατικό (κυβερνοεπίθεση) που θα απαιτούσε την εφαρμογή της εν λόγω διαδικασίας.

Το έγγραφο στοχεύει να είναι ένας πρακτικός οδηγός, που θα περιγράφει τα βήματα που θα πρέπει να ακολουθηθούν, όταν προκύψει ένα κυβερνο-περιστατικό, που με την σειρά του απαιτεί τη συλλογή των απαραίτητων αποδεικτικών στοιχείων, για τη διενέργεια της επακόλουθης ψηφιακής εγκληματολογικής ανάλυσης που οδηγεί στην αντιμετώπιση του περιστατικού. Αυτή η επακόλουθη ανάλυση είναι πέρα από το αντικείμενο του παρόντος εγγράφου.

Στον συγκεκριμένο οδηγό, θα χρησιμοποιηθούν εργαλεία που είναι ελεύθερα στο διαδίκτυο και δεν απαιτούν εμπορική άδεια.

ΤΜΗΜΑ 2
ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΟΙ ΣΥΜΒΟΛΙΣΜΟΙ

Οι ακόλουθοι συμβολισμοί θα χρησιμοποιηθούν στο έγγραφο:

Παράδειγμα Τμήματα ή μέρη του εγγράφου, που στόχο έχουν να πραγματοποιήσουν μια επίδειξη που να δείχνει πότε η παρεχόμενη πληροφορία θα μπορούσε να χρησιμοποιηθεί.

Σημαντικό Υπογραμμίζει ορισμένες πληροφορίες που είναι σημαντικές

και θα πρέπει να τύχουν ιδιαίτερης προσοχής.

Σημείωση Ενημερώνει για μια πτυχή-διάσταση που πρέπει να έχουμε κατά νου.

Άλλα εργαλεία Παρουσιάζει-προτείνει και άλλα εργαλεία με παρόμοια χαρακτηριστικά ή λειτουργίες σε σχέση με αυτό που προαναφέρθηκε στην προηγούμενη ενότητα.

ΚΕΦΑΛΑΙΟ «Β»
ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΑΝΑΛΥΣΗ

ΤΜΗΜΑ 3
ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΑΝΑΛΥΣΗ

Η έννοια της ψηφιακής εγκληματολογικής ανάλυσης αναφέρεται σε ένα συνδυασμό διαδικασιών συλλογής και ανάλυσης αποδεικτικών στοιχείων που διεξάγονται με σκοπό την αντιμετώπιση ενός κυβερνο-περιστατικού, που σχετίζεται με την ασφάλεια υπολογιστών και δικτύων και που -σε ορισμένες περιπτώσεις- μπορεί να χρησιμοποιηθεί ως αποδεικτικό στοιχείο στο δικαστήριο. Ο στόχος είναι να απαντήσουμε στο **τι, πού, πότε, γιατί, ποιος** και **πώς**, με την ολοκλήρωση αυτής της διαδικασίας. Ως ανάλυση ορίζουμε την συλλογή δεδομένων, την συσχέτιση μεταξύ τους και την ερμηνεία τους.

Η Ψηφιακή σήμανση (Digital forensics) είναι ένας κλάδος της σήμανσης που περιλαμβάνει την ανάκτηση και την έρευνα του ψηφιακού υλικού (που βρίσκεται σε ψηφιακές συσκευές), που έχει σχέση με το έγκλημα πληροφορικής (κυβερνοέγκλημα). (Wikipedia).

Αντικειμενικός σκοπός της ψηφιακής σήμανσης είναι, να παρουσιάσει τα αποδεδειγμένα γεγονότα, δηλαδή, να περιγράψει ακριβώς τι έγινε στο υπό εξέταση σύστημα.

Ο διαχειριστής συμβάντος θα πρέπει να περιγράψει ακριβώς τι έγινε, να πει την ιστορία, να δείξει το τι συνέβη, ενώ αντίθετα ο κακόβουλος χρήστης θέλει να επιτύχει το σκοπό του!

Αυτή η επιστήμη έχει αρχίσει να αποκτά έναν πολύ σημαντικό ρόλο τα τελευταία χρόνια, καθώς όλο και συχνότερα έχουμε να αντιμετωπίσουμε διαφορετικά κυβερνο-περιστατικά που σχετίζονται με την ασφάλεια των υπολογιστών, όπως παράνομες εισβολές σε υπολογιστές και δίκτυα, την υποκλοπή πληροφοριών, τις μολύνσεις από ιούς, κλπ.

Η χρήση της επεκτείνεται μέσω ποικίλων πεδίων, για παράδειγμα:

- Δίωξη ψηφιακών εγκλημάτων όπως παραβίαση συστημάτων (hacking), οικονομική απάτη, φοροδιαφυγή, παρενόχληση ή παιδική πορνογραφία.
- Περιπτώσεις διάκρισης ή παρενόχλησης.
- Έρευνα ασφάλισης.
- Ανάκτηση διαγραφέντων αρχείων.

- Κλοπή πνευματικής ιδιοκτησίας.
- Κυβερνοτρομοκρατία.
- Ενίσχυση της ανθεκτικότητας των επιχειρήσεων, ή με άλλα λόγια, η ικανότητα ανάκτησης από επιθέσεις.

Το πώς αντιμετωπίζονται οι διαφορετικές περιπτώσεις, θα αντικατοπτριστεί σε ολόκληρο το έγγραφο, καθώς είναι ζωτικής σημασίας να έχουμε μια σαφή ιδέα για τα βήματα που ακολουθούν κατά τη διενέργεια μιας ψηφιακής εγκληματολογικής ανάλυσης, ώστε να μην καταστρέψουμε αποδεικτικά στοιχεία που θα καταστήσουν αδύνατη την επίλυση του περιστατικού με έναν αποτελεσματικό τρόπο. Ένα περιστατικό έχει επιλυθεί με ικανοποιητικό τρόπο, όταν εξάγονται συμπεράσματα που δίνουν τη δυνατότητα να απαντήσουμε στις ερωτήσεις που αναφέρθηκαν προηγουμένως. Επίσης ένα περιστατικό έχει επιλυθεί σωστά, όταν ακολουθώντας την ίδια διαδικασία, καταλήγουμε στο ίδιο συμπέρασμα.

Στην περίπτωση της παραβίασης ενός υπολογιστή ή ενός δικτύου υπολογιστών ο αντικειμενικός σκοπός της ψηφιακής σήμανσης είναι:

- Να ανακαλύψουμε τη φύση και τον σκοπό του ιομορφικού λογισμικού
- Να καθορίσουμε το μηχανισμό μόλυνσης
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με τον μολυσμένο υπολογιστή.
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με το δίκτυο
- Να καθορίσουμε πως ο κακόβουλος χρήστης αλληλεπιδρά με το ιομορφικό πρόγραμμα
- Να καθορίσουμε το σκεπτικό και το σκοπό της κυβερνοεπίθεσης, καθώς και το επίπεδο, το σχεδιασμό της επίθεσης.
- Να καθορίσουμε την έκταση της μόλυνσης του προσωπικού υπολογιστή αλλά και την επέκταση της μόλυνσης στο δίκτυο.

Με την ψηφιακή εγκληματολογική ανάλυση μπορούμε να πετύχουμε αρκετά, όπως:

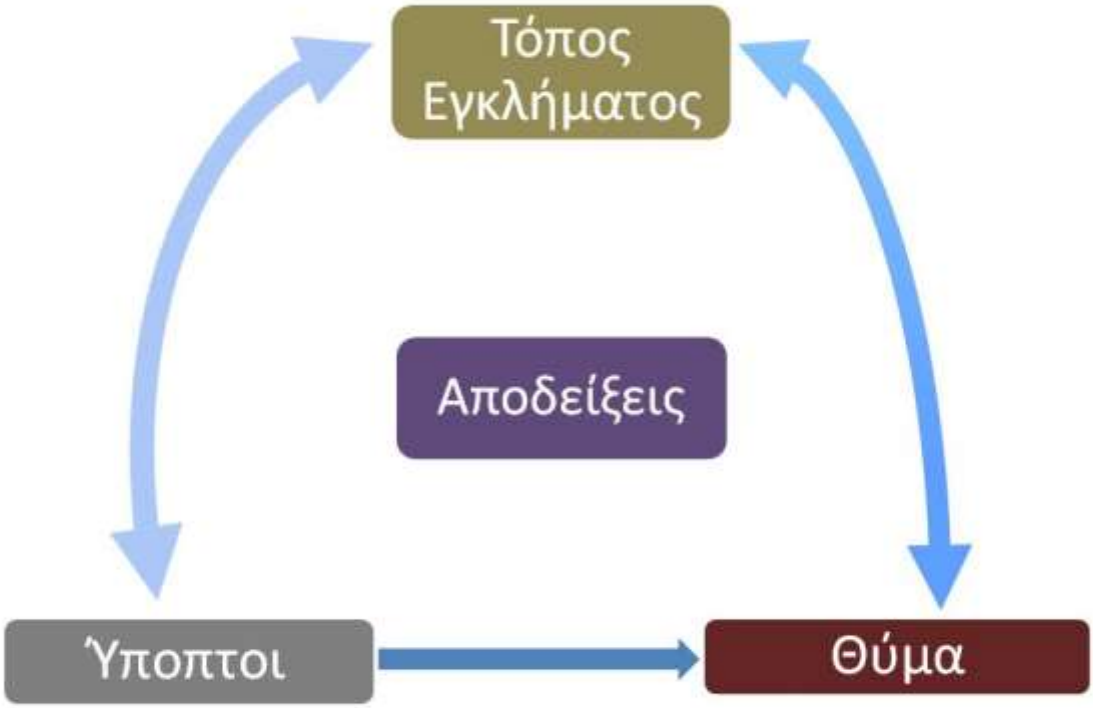
- Αποκατάσταση διαγραφέντων δεδομένων
- Αποκάλυψη πότε τα αρχεία τροποποιήθηκαν, δημιουργήθηκαν, διαγράφτηκαν.
- Μπορούμε να καθορίσουμε ποιες συσκευές τοποθετήθηκαν σε συγκεκριμένο υπολογιστή.
- Ποιες εφαρμογές εγκατασταθήκαν και από ποιον χρήστη.
- Ποιες ιστοσελίδες επισκεφτήκαμε.

Τι δεν μπορούμε να πετύχουμε:

- Εάν έχει καταστραφεί το αποθηκευτικό μέσο, δεν μπορούμε να κάνουμε αποκατάσταση δεδομένων.
- Εάν το αποθηκευτικό μέσο, έχει διαγραφεί με ασφαλή τρόπο, τότε δύσκολα έως αδύνατον να πετύχουμε αποκατάσταση δεδομένων.

ΤΜΗΜΑ 4
Η ΑΡΧΗ ΤΗΣ ΑΝΤΑΛΛΑΓΗΣ ΤΟΥ LOCARD

Κατά τη διενέργεια μιας ψηφιακής εγκληματολογικής ανάλυσης είναι ζωτικής σημασίας να έχουμε κατά νου την αρχή της ανταλλαγής του Locard. Ο Γάλλος εγκληματολόγος Edmond Locard είχε εκφράσει την άποψη πως είναι αδύνατον για έναν εγκληματία να δράσει χωρίς να αφήσει ίχνη της παρουσίας του. Μ' άλλα λόγια, πίστευε πως ο εγκληματίας θα αφήσει κάτι στον τόπο του εγκλήματος και ταυτόχρονα θα πάρει κάτι μαζί του. Αυτή είναι και η βασική αρχή της εγκληματολογικής επιστήμης, που έγινε γνωστή ως **αρχή της ανταλλαγής του Locard: Η επαφή μεταξύ δύο στοιχείων, πάντα θα επιφέρει μιαν ανταλλαγή.** Αυτό σημαίνει ότι κάθε είδος εγκλήματος, συμπεριλαμβανομένων εκείνων που σχετίζονται με την πληροφορική, που είναι και αυτό που μας αφορά, αφήνει ένα ίχνος, που σημαίνει ότι μέσα από μια διαδικασία εγκληματολογικής ανάλυσης είναι δυνατό να συγκεντρωθούν αποδεικτικά στοιχεία.



Εικόνα 1: Η αρχή της ανταλλαγής του Locard

Σημαντικό

Ομοίως, η αρχή της ανταλλαγής του Locard λαμβάνει χώρα και κατά τη διενέργεια της πραγματικής εγκληματολογικής ψηφιακής ανάλυσης, πράγμα που σημαίνει ότι θα πρέπει να είμαστε εξαιρετικά προσεκτικοί, έτσι ώστε το σύστημα να επηρεαστεί όσο το δυνατόν λιγότερο και τα αποκτηθέντα αποδεικτικά στοιχεία να μην μεταβληθούν.

ΤΜΗΜΑ 5
ΤΥΠΟΙ ΨΗΦΙΑΚΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΑΝΑΛΥΣΗΣ

Η ταξινόμηση των τύπων της ψηφιακής εγκληματολογικής ανάλυσης μπορεί να γίνει ανάλογα με το τι αυτή αποσκοπεί να αναλύσει (ποιο είναι το αντικείμενο). Έχοντας αυτό υπόψη είναι δυνατόν να προσδιοριστούν τέσσερις περιπτώσεις ανάλυσης:

- Εγκληματολογική ψηφιακή ανάλυση λειτουργικού συστήματος: όλα τα λειτουργικά συστήματα όπως Windows, GNU/Linux, OSX κλπ.
- Εγκληματολογική ψηφιακή ανάλυση δικτύου.
- Εγκληματολογική ψηφιακή ανάλυση ενσωματωμένου συστήματος.
- Εγκληματολογική ψηφιακή ανάλυση μνήμης (προσωρινής αποθήκευσης - volatile memory).

Ο οδηγός αυτός, όπως υποδηλώνει το όνομά του και έχει αναφερθεί προηγουμένως, εστιάζει στη συλλογή αποδεικτικών στοιχείων σε Linux λειτουργικά συστήματα, αν και η διαδικασία από μια γενικότερη άποψη είναι παρόμοια για όλους τους τύπους λειτουργικών συστημάτων.

ΤΜΗΜΑ 6
ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Η διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης πρέπει να κατέχει τα ακόλουθα χαρακτηριστικά:

- **Επαληθεύσιμη**: πρέπει να είναι δυνατόν να επιβεβαιωθεί η εγκυρότητα των συμπερασμάτων που προέκυψαν από την ανάλυση που διενεργήθηκε.

- **Αναπαράξιμη**: όλες οι δοκιμές που πραγματοποιήθηκαν καθ' όλη τη διαδικασία πρέπει να μπορούν να αναπαραχθούν ανά πάσα στιγμή.

- **Τεκμηριωμένη**: η όλη διαδικασία πρέπει να τεκμηριώνεται σωστά και πρέπει να πραγματοποιείται με κατανοητό και λεπτομερή τρόπο.

- **Ανεξάρτητη**: τα συμπεράσματα που προκύπτουν πρέπει να είναι τα ίδια, ανεξάρτητα από το πρόσωπο που διενεργεί τη διαδικασία και τη μέθοδο που χρησιμοποιείται.

ΤΜΗΜΑ 7
ΦΑΣΕΙΣ

Η διαδικασία της εγκληματολογικής ανάλυσης αποτελείται από τις ακόλουθες φάσεις:

Εικόνα 2: Οι φάσεις της διαδικασίας της εγκληματολογικής ανάλυσης

• **Διατήρηση**: Αντιστοιχεί στη φάση που εγγυάται ότι κανένα αποδεικτικό στοιχείο που έχει συλλεχθεί για μεταγενέστερη ανάλυση δεν θα χαθεί. Μία έλλειψη γνώσης, δηλαδή της ορθής διαδικασίας συλλογής πληροφοριών, θα μπορούσε να οδηγήσει σε απώλεια σχετικών πληροφοριών που θα μπορούσαν να είναι καθοριστικές για την επίλυση του κυβερνο-περιστατικού. Κρίσιμες ενέργειες όπως η μη απενεργοποίηση του συστήματος για να διατηρηθούν οι πληροφορίες προσωρινής αποθήκευσης (συλλογή μνήμης) ή η σωστή σήμανση των δεδομένων-στοιχείων που πρόκειται στην συνέχεια να αναλυθούν, λαμβάνουν χώρα κατά τη διάρκεια αυτής της φάσης.

Ομοίως, θα πρέπει να πραγματοποιείται μια σταθερή και συνεχόμενη καταγραφή όλων των ενεργειών που λαμβάνουν χώρα στο υλικό (στοιχεία) που πρόκειται να αναλυθεί. Σκοπός της καταγραφής είναι να διατηρηθεί η νομική εγκυρότητα των στοιχείων που συγκεντρώθηκαν, ώστε να αποδειχθούν όλα νόμιμα στην περίπτωση αντιδικίας. Αν τα δεδομένα (αποδεικτικά στοιχεία) χρειαστεί να μεταφερθούν, αυτό θα πρέπει να γίνει με τη μεγαλύτερη δυνατή προσοχή, αποφεύγοντας να αλλοιωθούν οι πληροφορίες ή να εκτεθούν σε ακραίες θερμοκρασίες (σκληροί δίσκοι) ή σε ηλεκτρομαγνητικά πεδία.

• **Απόκτηση-συλλογή**: Αυτή είναι η φάση με την οποία ασχολείται ο εν λόγω οδηγός. Η συγκεκριμένη φάση θα παρουσιαστεί με την μέγιστη λεπτομέρεια και που αντιστοιχεί στο στάδιο όπου συγκεντρώνονται τα αποδεικτικά στοιχεία. Ως αποδεικτικό στοιχείο μπορεί να οριστεί κάθε απόδειξη που μπορεί να χρησιμοποιηθεί σε μια νομική διαδικασία, αν και αυτό δεν είναι πάντα η υπόθεση.

Χαρακτηριστικά των αποδεικτικών στοιχείων:

- **Παραδεκτά**: πρέπει να έχουν νομική αξία.

- **Αυθεντικά**: πρέπει να είναι αληθή και να μην χειραγωγούνται-αλλοιώνονται με οποιοδήποτε τρόπο. Για το σκοπό αυτό, πρέπει να έχουν εξαχθεί τα αντίστοιχα αποτελέσματα των αλγορίθμων κατακερματισμού (hashes - ελέγχου ακεραιότητας) για να εξασφαλίζεται η ακεραιότητά τους.

- **Ολοκληρωμένα**: πρέπει να παρουσιάζουν τα αποδεικτικά στοιχεία από μια αντικειμενική και τεχνική άποψη, χωρίς προσωπικές εκτιμήσεις ή προκαταλήψεις.

- **Σαφή**: πρέπει να είναι κατανοητά.

- **Αξιόπιστα**: οι τεχνικές που χρησιμοποιούνται για τη συγκέντρωση αποδεικτικών στοιχείων δεν πρέπει να δημιουργούν αμφιβολίες ως προς την ειλικρίνεια και την αυθεντικότητα τους.

Μπορούν να ταξινομηθούν σε δύο τύπους:

• Φυσικά αποδεικτικά στοιχεία: αναφέρονται στα υλικά του

υπολογιστή όπως σκληροί δίσκοι, pen drives, κλπ.

• Ψηφιακά αποδεικτικά στοιχεία: αντιστοιχούν στις πληροφορίες που αποθηκεύονται στα ηλεκτρονικά αποδεικτικά στοιχεία.

Μερικά παραδείγματα των ψηφιακών αποδεικτικών στοιχείων είναι:

- Τα ψηφιακά αρχεία.
- Οι Διεργασίες/υπηρεσίες.
- Τα μητρώα καταγραφής συμβάντων (Log files).
- Τα προσωρινά αρχεία (Temporary files).
- Οι καταχωρήσεις – εγγραφές στην registry.

• **Ανάλυση**: Κατά τη διεξαγωγή της ανάλυσης των συλλεχθέντων πληροφοριών πρέπει να έχουμε κατά νου το συγκεκριμένο τύπο του περιστατικού για να ενεργήσουμε αντίστοιχα. Δηλαδή διαφορετικές είναι οι ενέργειες στην περίπτωση παράνομης διείσδυσης σε έναν υπολογιστή και διαφορετική στην περίπτωση παιδικής πορνογραφίας. Ανάλογα με την περίπτωση, μπορεί να είναι χρήσιμο να κάνουμε μία σε βάθος ανάλυση διαφορετικών αντικειμένων όπως:

- **Μνήμη (Memory):** Η μνήμη είναι ηλεκτρονικά κυκλώματα, τα οποία «αποθηκεύουν» προγράμματα και δεδομένα για να χρησιμοποιηθούν από τον μικροεπεξεργαστή. Υπάρχουν δύο είδη μνήμης. Η μνήμη ROM (Read Only Memory) και η μνήμη RAM (Random Access Memory). Χαρακτηριστικό μέγεθος της μνήμης είναι και πάλι η χωρητικότητα, η οποία μετριέται με τις ίδιες μονάδες μέτρησης, όπως και η χωρητικότητα του σκληρού δίσκου.

- **Κάδος ανακύκλωσης**.

- **Unassigned space (Μη εκχωρημένος χώρος)**: αντιστοιχεί στον ελεύθερο χώρο του δίσκου που διατίθεται για την αποθήκευση πληροφοριών. Όταν ένα αρχείο διαγράφεται στο Linux, το λειτουργικό σύστημα αφαιρεί μόνο την αναφορά στις εν λόγω πληροφορίες, αλλά όχι την ίδια την πληροφορία. Αντ' αυτού, η αντίστοιχη περιοχή στο δίσκο χαρακτηρίζεται ως ελεύθερη-εγγράψιμη. Ως εκ τούτου, οι διαγραμμένες πληροφορίες μπορούν να ανακτηθούν με διαφορετικά μέσα.

- **Slack Space**: αναφέρεται στον ελεύθερο χώρο που παραμένει μέσα σε ένα cluster (σετ των διπλανών τομέων του δίσκου που συνθέτουν τη μικρότερη μονάδα πληροφορίας σε ένα δίσκο) μετά την αποθήκευση ενός αρχείου.

- **Κίνηση του δικτύου**.

- **Διεργασίες του συστήματος**.

- **Μητρώα καταγραφής συμβάντων του συστήματος (Log files)**: όπως τα αρχεία καταγραφής των συμβάντων που σχετίζονται με το σύστημα, την ασφάλεια ή τις εφαρμογές.

Είναι ζωτικής σημασίας η όλη διαδικασία να διενεργείται με αντικειμενική άποψη, χωρίς να αποκλείεται αυτό που ο αναλυτής μπορεί να θεωρήσει προφανές.

• **Τεκμηρίωση:** Μια θεμελιώδη διάσταση στη διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης είναι η τεκμηρίωση. Η συγκεκριμένη φάση θα πρέπει να πραγματοποιείται με ένα πολύ μεθοδικό και λεπτομερή τρόπο. Οι ακόλουθες ενέργειες, μεταξύ άλλων, μπορούν να χρησιμοποιηθούν-πραγματοποιηθούν:

- Φωτογραφίζουμε τις αποδείξεις.
- Διατηρούμε την αλυσίδα παρακολούθησης-επιτήρησης (chain of custody).
- Καταγράφουμε κάθε βήμα που λαμβάνεται κατά τη διάρκεια της διαδικασίας, κρατώντας ένα αρχείο καταγραφής με τις ημερομηνίες και τις ώρες κάθε ενέργειας που πραγματοποιείται στο αποδεικτικό στοιχείο.
- Εκπονούμε δύο τύπους για τις αναφορές συμπερασμάτων: έναν εκτελεστικό (περιληπτικό) και έναν τεχνικό.

• **Παρουσίαση**: Η παρουσίαση των πληροφοριών είναι εξίσου σημαντική καθώς τα συμπεράσματα που εξάγονται κατά την διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης θα πρέπει να είναι προσβάσιμα και απόλυτα κατανοητά.

Για να το επιτύχουμε αυτό αυτό, θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

- Ετοιμάζουμε μια παρουσίαση με έναν εκπαιδευτικό τρόπο, ώστε να είναι εύκολα κατανοητή.
- Περιγράφουμε λεπτομερώς τα συμπεράσματα.
- Εξηγούμε με σαφήνεια τη διαδικασία που έχει ακολουθηθεί για την απόκτηση των αποδεικτικών στοιχείων.
- Αποφεύγουμε τις μη-αποδείξιμες επιβεβαιώσεις ή υποκειμενικές κρίσεις.
- Εκπονούμε-παρουσιάζουμε τα συμπεράσματα από μια αντικειμενική άποψη.

Θα πρέπει να σημειωθεί ότι οι φάσεις δεν είναι διαδοχικές αλλά επαναλαμβανόμενες και διαπλεκόμενες. Για παράδειγμα, η φάση της τεκμηρίωσης αρχίζει κατά τη διάρκεια της φάσης της διατήρησης.

ΤΜΗΜΑ 8
ΜΕΘΟΔΟΙ ΚΑΙ ΟΔΗΓΟΙ

Υπάρχουν διάφορες μέθοδοι και οδηγοί κατά την εκτέλεση μιας ψηφιακής εγκληματολογικής ανάλυσης, αλλά όλα έχουν κοινές πτυχές.

Παρακάτω είναι μια άλλη σειρά οδηγών που θα μπορούσαν να χρησιμοποιηθούν ως σημείο αναφοράς για αναγνώστες που ενδιαφέρονται να ψάξουν περαιτέρω το θέμα:

• *Guidelines for the best practices in the forensic examination of digital*

technology[1]

• *Electronic Crime Scene Investigation: A Guide for First Responders*[2]

• *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*[3]

Μία γενικότερη προσέγγιση-μέθοδος της ψηφιακής εγκληματολογικής ανάλυσης θα μπορούσαν να αποτελέσουν τα παρακάτω βήματα:

1. Επιβεβαίωση συμβάντος (Verification)
2. Περιγραφή συστήματος (System description)
3. Συλλογή δεδομένων (Evidence Acquisition)
4. Χρονική ανάλυση δεδομένων (Timeline Analysis)
5. Ανάλυση συσκευών αποθήκευσης (Media analysis)
6. Αλφαριθμική αναζήτηση ή αναζήτηση κατά Byte
7. Αποκατάσταση δεδομένων (Data Recovery)
8. Αναφορά (Reporting)

Στον συγκεκριμένο οδηγό θα παρουσιάσουμε το τρίτο βήμα που αφορά την συλλογή δεδομένων, ενώ θα αναφερθούμε και στα δύο πρώτα, που αφορούν επιβεβαίωση συμβάντος και περιγραφή συστήματος.

Μία ακόμα γενική προσέγγιση περιγραφής βημάτων της ψηφιακής εγκληματολογικής ανάλυσης είναι και η ακόλουθη:

Φάση 1: Ανάκτηση, Διατήρηση (σωστή διαδικασία φύλαξης/επιμέλειας -chain of custody-) και εξέταση των πτητικών δεδομένων

Φάση 2: Ανάλυση της μνήμης

Φάση 3: Ανάλυση ψηφιακής σήμανσης: εξέταση των αποθηκευτικών μέσων

Φάση 4: Εντοπισμός και ανάλυση αγνώστων αρχείων

Φάση 5: Δυναμική και στατική ανάλυση ιομορφικού λογισμικού.

Εμείς θα επικεντρωθούμε στην πρώτη φάση: Ανάκτηση, Διατήρηση (σωστή διαδικασία φύλαξης-επιμέλειας -chain of custody) και εξέταση των πτητικών δεδομένων με μία σύντομη ανάλυση της φάσης 3.

[1] http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html

[2] https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[3] https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

ΚΕΦΑΛΑΙΟ «Γ»
ΚΥΒΕΡΝΟ-ΠΕΡΙΣΤΑΤΙΚΑ

ΤΜΗΜΑ 9
ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΕΝΟΣ ΚΥΒΕΡΝΟ-ΠΕΡΙΣΤΑΤΙΚΟΥ

Υπάρχει μια πληθώρα περιστατικών που σχετίζονται με την παραβίαση της ασφάλειας υπολογιστών και δικτύων:

Λαμβάνοντας υπόψη τα κυβερνο-περιστατικά που πιθανών να κληθεί κάποιος επαγγελματίας να αντιμετωπίσει, αυτά μπορούν να προσδιοριστούν στις ακόλουθες περιπτώσεις:

- **Κλοπή πληροφοριών**: Η κλοπή προσωπικών ή πληροφοριών μιας επιχείρησης, είναι μία από τις σημαντικότερες ανησυχίες τόσο για τους χρήστες όσο και για τις επιχειρήσεις. Υπάρχουν μια σειρά από τεχνικές που επιτρέπουν την κλοπή πληροφοριών, όπως η παρακολούθηση της κυκλοφορίας του δικτύου μέσω **sniffer**, η υποκλοπή των emails ή απλά η σύνδεση μιας συσκευής **usb** για αντιγραφή ιδιωτικών πληροφοριών, κλπ. Αυτές οι πληροφορίες χρησιμοποιούνται κυρίως για οικονομικό όφελος, αλλά σε ορισμένες περιπτώσεις, απλώς χρησιμοποιούνται για να βλάψουν την εικόνα του θιγόμενου μέρους.

- **Απάτη**: Υπάρχει ένας αριθμός παραδειγμάτων Διαδικτυακής Απάτης, όπως:

  - Ψευδείς προσφορές εργασίας.
  - Απάτες λοταρίας και βραβείων.
  - Ψευδείς κληρονομιές.
  - Απάτες επενδύσεων και πιστώσεων.
  - Ψευδή emails που ζητούν δωρεές σε Μη Κυβερνητικές

Οργανώσεις.

- Πλαστά τιμολόγια από υπηρεσίες μηνυμάτων.
- Μεταφορτώσεις τιμολόγιων από υπηρεσίες SMS.
- Πρόστιμα για παράνομες λήψεις (μεταφορτώσεις δεδομένων).

Καθ' όλη τη διάρκεια του χρόνου, ένας μεγάλος αριθμός παράνομων ενεργειών λαμβάνουν χώρα, αξιοποιώντας στο έπακρο τις σημαντικές ημερομηνίες ή τα γεγονότα, για να πολλαπλασιάσουν αυτά τα είδη των απειλών.

- **Ιομορφικό λογισμικό**: Το ιομορφικό λογισμικό είναι άλλο ένα από τα πιο χαρακτηριστικά περιστατικά που ένας αναλυτής ψηφιακού εγκλήματος μπορεί να συναντήσει. Η επαγγελματοποίηση της αγοράς έχει δημιουργήσει μια σημαντική αύξηση του όγκου αυτών των ειδών των απειλών, φθάνοντας σε πολύ εξελιγμένα επίπεδα σε ορισμένες περιπτώσεις. Το 2017 ένα νέο δείγμα ιομορφικού λογισμικού παρουσιάζεται κάθε 4.2 δευτερόλεπτα. Η πιο δημοφιλής κατηγορία ιομορφικού λογισμικού είναι οι δούρειοι ίπποι (Trojan horse) οι οποίοι εκτελούν διάφορες κακόβουλες δραστηριότητες όπως κατέβασμα αρχείων, spyware, keyloggers και κλοπείς κωδικών πρόσβασης, συμμετοχή σε botnets και διεξαγωγή κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης (DDoS).

Η κυρίαρχη πλατφόρμα που στοχεύει το ιομορφικο λογισμικό εξακολουθεί να είναι τα Windows. Καλύπτει το 99,1% του δείγματος. Παρόλα αυτά ο τεράστιος αριθμός τους αποτελεί απειλή και για τα άλλα λειτουργικά συστήματα όπως το OSX, το Android και το Unix/Linux.

Στην περίπτωση που έχουμε μόλυνση με ιομορφικό λογισμικό, τότε ο αντικειμενικός σκοπός της ψηφιακής σήμανσης είναι:

- Να ανακαλύψουμε την φύση και τον σκοπό του ιομορφικού λογισμικού
- Να καθορίσουμε τον μηχανισμό μόλυνσης
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με τον μολυσμένο υπολογιστή.
- Να καθορίσουμε πως το ιομορφικό πρόγραμμα αλληλεπιδρά με το δίκτυο
- Να καθορίσουμε πως ο κακόβουλος χρήστης αλληλεπιδρά με το ιομορφικό πρόγραμμα
- Να καθορίσουμε το σκεπτικό και το σκοπό της κυβερνοεπίθεσης, καθώς και το επίπεδο, το σχεδιασμό της επίθεσης.
- Να καθορίσουμε την έκταση της μόλυνσης του προσωπικού υπολογιστή αλλά και την επέκταση της μόλυνσης στο δίκτυο

- **Μη-εξουσιοδοτημένη πρόσβαση**: Σύμφωνα με μία μελέτη του ThreatTrack Security, η μη-εξουσιοδοτημένη πρόσβαση σε δικτυακούς τόπους με σεξουαλικό περιεχόμενο είναι ένας από τους κύριους λόγους μόλυνσης των εταιρικών υπολογιστών. Ένα άλλο παράδειγμα είναι η εκμετάλλευση τρωτοτήτων του λογισμικού για την απόκτηση προνομίων και πρόσβασης σε φακέλους και έγγραφα που περιέχουν εμπιστευτικές πληροφορίες.

- **Μη ορθή χρήση πόρων**: Η μη ορθή χρήση των πόρων είναι μία αρκετά συνήθης πρακτική στις επιχειρήσεις που μπορεί να τις εκθέσουν. Η εκτύπωση προσωπικών εγγράφων είναι ένα από τα πιο χαρακτηριστικά παραδείγματα.

- **Πνευματική ιδιοκτησία**: Η παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας έχει ως αποτέλεσμα ένα πολύ σημαντικό ετήσιο κόστος. Σύμφωνα με μια μελέτη για τις οικονομικές επιπτώσεις της εγκληματικότητας στον κυβερνοχώρο από τη McAfee, αυτό προκαλεί, σε παγκόσμιο επίπεδο, ζημίες μέχρι 400.000 εκατομμύρια δολάρια και ένας από τους κύριους λόγους είναι η κλοπή της πνευματικής ιδιοκτησίας. Υπάρχει ένας τεράστιος αριθμός ιστοσελίδων όπου μπορούμε να μεταφορτώσουμε ταινίες, μουσική, λογισμικό, κλπ, τα οποία έχουν άμεσο αντίκτυπο σε αυτές τις απώλειες.

- **Άρνηση παροχής υπηρεσιών (Denial-of-service)**: Μια επίθεση άρνησης παροχής υπηρεσιών στοχεύει να εμποδίσει την πρόσβαση σε υπηρεσίες και πόρους ενός οργανισμού. Αυτά τα είδη των επιθέσεων συνήθως διαπράττονται μέσω της χρήσης των botnets (δίκτυα μολυσμένων υπολογιστών) ή με την εκμετάλλευση αδυναμιών των υπηρεσιών και έχουν αυξηθεί σημαντικά τα τελευταία χρόνια, μερικές φορές προκαλούνται από ενέργειες χακτιβιστών (hacktivist actions).

Παρά την ποικιλομορφία των κυβερνο-περιστατικών, η διαδικασία που ακολουθείται κατά τη συγκέντρωση των αποδεικτικών στοιχείων είναι κοινή στην πλειονότητα των περιπτώσεων. Πρέπει να έχουμε κατά νου ότι η ανάλυση που ακολουθεί, θα είναι συγκεκριμένη και διαφορετική, ανάλογα με τον τύπο του κυβερνο-περιστατικού.

Υπάρχουν και άλλα είδη περιστατικών, που σχετίζονται κυρίως με την παιδική πορνογραφία, κυβερνοτρομοκρατία, εκβιασμούς (η ομάδα αυτή περιλαμβάνει την παρενόχληση στον κυβερνοχώρο -cyberharassment-), τον εκφοβισμό στον κυβερνοχώρο (cyberbullying), η αποπλάνηση ανηλίκου, το sexting ή την σεξουαλική παρενόχληση (intimacy infringement)], κλπ, τα οποία πρέπει να διαβιβάζονται στις αρμόδιες αρχές για να ξεκινούν την έρευνα και να λαμβάνουν τα μέτρα που κρίνουν κατάλληλα. Αυτά τα είδη των περιστατικών είναι πέρα από το αντικείμενο του συγκεκριμένου οδηγού. Στην πραγματικότητα, μερικά από τα περιστατικά που περιγράφονται σε αυτό το σημείο μπορεί να απαιτούν τη διαβίβασή τους στις αρχές, όπως εκείνα που σχετίζονται με την κλοπή πληροφοριών ή την απάτη. Για όλα αυτά θα πρέπει να ερχόμαστε σε επαφή με την Δίωξη Ηλεκτρονικού Εγκλήματος και να ακολουθούμε τα βήματα που θα μας υποδείξουν.

ΚΕΦΑΛΑΙΟ «Δ»
ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΟΔΗΓΙΕΣ ΓΙΑ ΤΗ ΣΥΛΛΟΓΗ ΚΑΙ ΑΠΟΘΗΚΕΥΣΗ ΤΩΝ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Το **RFC 3227**[4] είναι ένα έγγραφο που περιλαμβάνει τις «*κατευθυντήριες γραμμές για τη συλλογή και αποθήκευση αποδεικτικών στοιχείων*» και μπορεί να χρησιμοποιηθεί ως πρότυπο για τη συλλογή πληροφοριών σε περιστατικά ασφαλείας.

Το έγγραφο περιλαμβάνει τις παρακάτω ενότητες:

ΤΜΗΜΑ 10
ΑΡΧΕΣ ΚΑΤΑ ΤΗ ΣΥΓΚΕΝΤΡΩΣΗ ΤΩΝ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

- Ανακτούμε ένα ακριβές αντίγραφο του συστήματος που θα είναι όσο το δυνατόν πιο πιστό αντίγραφο.
- Κρατούμε λεπτομερείς σημειώσεις, συμπεριλαμβανομένων ημερομηνιών και ωρών που αναγράφονται εάν χρησιμοποιείται η τοπική ή η παγκόσμια (UTC) ώρα.
- Ελαχιστοποιούμε τις αλλαγές στις πληροφορίες που έχουν συγκεντρωθεί και εξαλείφουμε εξωτερικούς παράγοντες που μπορεί να πραγματοποιήσουν αλλαγές.
- Αν αντιμετωπίζουμε ένα δίλημμα μεταξύ συλλογής και ανάλυσης, επιλέγουμε πρώτα συλλογή και δεύτερον ανάλυση.
- Συγκεντρώνουμε τις πληροφορίες ανάλογα με τη σειρά της πτητικότητας/μεταβλητότητας (από τις περισσότερο στις λιγότερο μεταβλητές).
- Λαμβάνουμε υπόψιν ότι με κάθε συσκευή η συλλογή πληροφοριών μπορεί να πραγματοποιηθεί με έναν διαφορετικό τρόπο.

<u>Η σειρά μεταβλητότητας (Volatility order)</u>

Η σειρά μεταβλητότητας αναφέρεται στο χρονικό διάστημα κατά το οποίο ορισμένες πληροφορίες είναι προσβάσιμες. Ως εκ τούτου, είναι απαραίτητο να συγκεντρωθούν πρώτες οι πληροφορίες που πρόκειται να είναι διαθέσιμες για τον ελάχιστο χρόνο, με άλλα λόγια, οι πληροφορίες με τη μεγαλύτερη μεταβλητότητα.

Ακολουθώντας αυτή την σειρά, μπορεί να δημιουργηθεί η ακόλουθη λίστα από το περισσότερο στο λιγότερο μεταβλητό:

- Περιεχόμενα φυσικής μνήμης (physical memory).
- Διευθύνσεις IP, λεπτομέρειες λειτουργικού συστήματος.
- Κατάσταση συστήματος και λεπτομέρειες περιβάλλοντος.
- Δίσκος.
- Αρχεία καταγραφής συστήματος.
- Έγγραφα.

[4] https://www.ietf.org/rfc/rfc3227.txt

Ενέργειες που πρέπει να αποφεύγονται

Οι παρακάτω ενέργειες πρέπει να αποφεύγονται για να μην ακυρώσουν τη διαδικασία συλλογής πληροφοριών, δεδομένου ότι πρέπει να διατηρηθεί η ακεραιότητά τους, έτσι ώστε τα λαμβανόμενα αποτελέσματα να μπορούν να χρησιμοποιηθούν στο δικαστήριο, εάν χρειαστεί:

- Δεν απενεργοποιούμε τον υπολογιστή μέχρι να συλλεχθούν όλες οι μεταβλητές-πτητικές πληροφορίες.
- Δεν εμπιστευόμαστε τις πληροφορίες που παρέχονται από το λογισμικό του συστήματος, καθώς ενδέχεται να έχει μολυνθεί. Οι πληροφορίες πρέπει να συλλέγονται μέσω λογισμικού που είναι αποθηκευμένο σε ένα προστατευμένο μέσο (USB, CD-ROM), όπως θα εξηγηθεί στη συνέχεια.
- Δεν εκτελούμε λογισμικό που τροποποιεί την ημερομηνία και την ώρα της πρόσβασης όλων των αρχείων του συστήματος.

Θέματα προστασίας προσωπικών δεδομένων (Privacy considerations)

Όλες οι πληροφορίες που συγκεντρώθηκαν κατά τη διάρκεια της διαδικασίας, θα πρέπει να είναι εγγυημένο πως θα αντιμετωπίζονται μέσα στο θεσπισμένο νομικό πλαίσιο, διατηρώντας την απαιτούμενη προστασία προσωπικών δεδομένων. Τα αρχεία καταγραφής συμβάντων περιλαμβάνονται σε αυτό το πλαίσιο προστασίας προσωπικών δεδομένων, καθώς μπορούν να αποθηκεύουν τα μοτίβα συμπεριφοράς του χρήστη του συστήματος.

Νομικά ζητήματα/σκέψεις (Legal considerations)

Πρέπει να σημειωθεί πως ο νόμος είναι διαφορετικός σε κάθε χώρα, έτσι τα αποδεικτικά στοιχεία μπορούν να γίνουν αποδεκτά σε μία χώρα και σε μία άλλη όχι. Σε κάθε περίπτωση, τα αποδεικτικά στοιχεία πρέπει να έχουν μια σειρά από κοινά χαρακτηριστικά.

- **Αποδεκτά**: η ισχύουσα νομοθεσία πρέπει να γίνεται σεβαστή για να έχουν τα αποδεικτικά στοιχεία μια δικαστική αξία.
- **Αυθεντικά**: πρέπει να είναι ευαπόδεικτο ότι τα αποδεικτικά στοιχεία αντιστοιχούν στο εν λόγω περιστατικό.
- **Ολοκληρωμένα**: πρέπει να αντιστοιχούν στο σύνολο των πληροφοριών και όχι απλώς σε μια μερική άποψη.
- **Αξιόπιστα**: δεν πρέπει να υπάρχουν αμφιβολίες ως προς το πώς προέκυψαν τα αποδεικτικά στοιχεία ή σχετικά με οποιοδήποτε μεταγενέστερο χειρισμό που θα μπορούσαν να εγείρουν αμφιβολίες σχετικά με την αυθεντικότητα και την ειλικρίνειά τους.
- **Αξιόπιστα/Σαφή**: πρέπει να είναι εύλογα και εύκολα κατανοητά για τον δικαστή στο δικαστήριο.

ΤΜΗΜΑ 11
ΔΙΑΔΙΚΑΣΙΑ ΣΥΛΛΟΓΗΣ

Η διαδικασία συλλογής πρέπει να είναι όσο το δυνατόν **πιο λεπτομερής**, εξασφαλίζοντας ότι δεν είναι διφορούμενη, δεν εμφανίζονται διλήμματα που θα απαιτούν αποφάσεις με λίγα λόγια επιδιώκουμε την μείωση/ αποφυγή λήψης αποφάσεων όσο το δυνατόν περισσότερο. Οι μέθοδοι που χρησιμοποιούνται για τη συλλογή των αποδεικτικών στοιχείων πρέπει να είναι διαφανείς και **αναπαράξιμες**. Θα πρέπει να είμαστε έτοιμοι να αναπαράξουμε με ακρίβεια τις μεθόδους που χρησιμοποιήθηκαν, και οι μέθοδοι αυτές πρέπει να έχουν ελεγχθεί από ανεξάρτητους εμπειρογνώμονες.

Βήματα

- Που είναι τα αποδεικτικά στοιχεία; Κάνουμε μια λίστα των συστημάτων που εμπλέκονται στο περιστατικό και αυτών που μπορούν να χρησιμοποιηθούν για την εξαγωγή στοιχείων.
- Καθορίζουμε τι είναι σχετικό. Σε περίπτωση αμφιβολίας, είναι καλύτερο να συγκεντρώσουμε περισσότερες πληροφορίες παρά ελλειπείς.
- Ορίζουμε τη σειρά μεταβλητότητας για κάθε σύστημα.
- Συλλέγουμε τις πληροφορίες σύμφωνα με την καθορισμένη σειρά.
- Επιβεβαιώνουμε το επίπεδο συγχρονισμού του ρολογιού του συστήματος.
- Καθώς γίνονται τα βήματα συλλογής αναρωτιόμαστε τι επιπλέον θα μπορούσε να αποτελέσει αποδεικτικό στοιχείο.
- Καταγράφουμε κάθε μας βήμα.
- Δεν ξεχνάμε τους ανθρώπους που εμπλέκονται. Σημειώνουμε ποιοι ήταν εκεί, τι έκαναν, τι έψαχναν και πως αντέδρασαν.

ΤΜΗΜΑ 12
Η ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΑΠΟΘΗΚΕΥΣΗΣ

Αλυσίδα παρακολούθησης

Η αλυσίδα παρακολούθησης πρέπει να τεκμηριώνεται/καταγράφεται σαφώς και τα ακόλουθα σημεία να προσδιορίζονται με λεπτομέρεια:

- Που, πότε και ποιος ανακάλυψε και συγκέντρωσε τα αποδεικτικά στοιχεία;
- Που, πότε και ποιος χειρίστηκε τα αποδεικτικά στοιχεία;
- Ποιος φύλαγε τα αποδεικτικά στοιχεία; Για πόσο καιρό; Και πώς τα αποθήκευε;
- Εάν τα αποδεικτικά στοιχεία άλλαξαν επιμέλεια / χέρια φύλαξης/παρακολούθησης, θα πρέπει να υποδείξουμε πότε και πώς έλαβε χώρα η ανταλλαγή, συμπεριλαμβανομένου του αριθμού δελτίου παράδοσης, κλπ.

Που και πώς αποθηκεύουμε τις πληροφορίες

Οι πληροφορίες πρέπει να αποθηκεύονται σε συσκευές με ένα επίπεδο

ασφάλειας που έχει αποδειχθεί και που μπορεί να ανιχνεύσει μη εξουσιοδοτημένες απόπειρες πρόσβασης. Τα δεδομένα θα πρέπει να μεταφερθούν σε ένα εξωτερικό αποθηκευτικό μέσο, με συγκεκριμένη σειρά, ξεκινώντας από την μνήμη και πραγματοποιώντας συνεχώς έλεγχο ακεραιότητας. Τα πρώτα δεδομένα που συλλέγουμε στην περίπτωση που το σύστημα είναι ενεργό, είναι τα δεδομένα που θα χαθούν μόλις τεθεί εκτός λειτουργίας ο υπολογιστής (π.χ μνήμη).

ΤΜΗΜΑ 13
ΑΠΑΡΑΙΤΗΤΑ ΕΡΓΑΛΕΙΑ

Υπάρχει μια σειρά από κατευθυντήριες γραμμές που πρέπει να ακολουθούνται κατά την επιλογή των εργαλείων που πρόκειται να χρησιμοποιηθούν για τη διαδικασία της συλλογής:

- Εργαλεία που είναι εξωτερικά (εκτός συστήματος) από το σύστημα θα πρέπει να χρησιμοποιούνται, διότι θεωρούμε δεδομένο πως τα αντίστοιχα εργαλεία του συστήματος έχουν μολυνθεί.
- Θα πρέπει να χρησιμοποιούνται εργαλεία που αλλάζουν την υπόθεση – περιστατικό όσο το δυνατόν λιγότερο. Συγκεκριμένα, να αποφεύγουμε, όταν είναι δυνατό, τη χρήση των εργαλείων γραφικού περιβάλλοντος και των εργαλείων με μεγάλη κατανάλωση μνήμης.
- Το λογισμικό που πρόκειται να χρησιμοποιηθεί για τη συγκέντρωση αποδεικτικών στοιχείων πρέπει να βρίσκεται σε μία εξωτερική συσκευή ανάγνωσης (CD-ROM, USB, κλπ).
- Ένας συνδυασμός εργαλείων, κατάλληλων για τα λειτουργικά συστήματα-στόχους θα πρέπει να είναι έτοιμος από πριν και να έχουν προ-ελεγχθεί.
- Η εργαλειοθήκη ανάλυσης θα πρέπει να περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα είδη εργαλείων:
  - Λογισμικό για την καταγραφή και εξέταση των διαδικασιών.
  - Λογισμικό για την εξέταση της κατάστασης του συστήματος.
  - Λογισμικό για να πραγματοποιεί αντίγραφα σε χαμηλό επίπεδο, δηλαδή **bit by bit**.

ΤΜΗΜΑ 14
ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά τη διεξαγωγή της διαδικασίας συλλογής πληροφοριών σε ένα σύστημα που έχει υποστεί ένα περιστατικό ασφαλείας, είναι απαραίτητο να έχουμε μια σαφή ιδέα για το τι ενέργειες πρέπει να διεξαχθούν, όντας πολύ σχολαστικοί και καταγράφοντας λεπτομερώς αυτή τη διαδικασία ανά πάσα στιγμή. Επομένως, η διαδικασία πρέπει να διεξαχθεί προσπαθώντας να είναι όσο το δυνατόν πιο διακριτική, προκειμένου να διατηρηθεί το σύστημα στην αρχική του κατάσταση (ή με τις ελάχιστες αλλαγές που ωστόσο μπορούμε να τις τεκμηριώσουμε).

ΚΕΦΑΛΑΙΟ «Ε»
ΣΥΓΚΕΝΤΡΩΣΗ ΑΠΟΔΕΙΚΤΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Ένα από τα κύρια καθήκοντα – απαιτήσεις, κατά τη διενέργεια ψηφιακής εγκληματολογικής ανάλυσης, είναι να έχουμε μια σαφή ιδέα για το συγκεκριμένο είδος του κυβερνο-περιστατικού και στην συνέχεια να γνωρίζουμε τι πληροφορίες είναι απαραίτητες να συλλέξουμε και πώς θα προχωρήσουμε. Υπάρχουν κοινές διαδικασίες, αλλά δεν είναι το ίδιο να πραγματοποιούμε μια ψηφιακή εγκληματολογική ανάλυση σε μια περίπτωση ιομορφικού λογισμικού από ότι σε μια υπόθεση απάτης, δεδομένου ότι τα σημεία που ο ερευνητής πρέπει να επικεντρωθεί για να εντοπίσει αποδεικτικά στοιχεία είναι διαφορετικά.

Προφανώς, μερικά από τα βήματα που υποδεικνύονται προηγουμένως μπορεί να μην είναι απαραίτητα, όπως το να πρέπει να παρουσιάσουμε αποδεικτικά στοιχεία στο δικαστήριο, έτσι ώστε τελικά η τεκμηρίωση να μην πρέπει να είναι τόσο πολύ εξαντλητική, ωστόσο συνιστάται να διεξαχθεί η διαδικασία από μία επαγγελματική και αναπόσπαστη άποψη και για αυτό να είναι όσο το δυνατόν πληρέστερη. Εναπόκειται στον αναγνώστη να καθορίσει ποιες πτυχές θα λάβει υπόψη του, ανάλογα με την κατάσταση που θα πρέπει να αναλύσει, και ποια βήματα θα ακολουθήσει.

ΤΜΗΜΑ 15
ΖΗΤΗΜΑΤΑ/ΕΞΕΤΑΣΕΙΣ/ΣΚΕΨΕΙΣ ΠΡΙΝ ΤΗΝ ΣΥΛΛΟΓΗ

Υπάρχουν μια σειρά από ζητήματα/εξετάσεις/σκέψεις που πρέπει να έχουμε κατά νου πριν από την έναρξη της διαδικασίας συλλογής αποδεικτικών στοιχείων:

- Αρχικά, δεν αγγίζουμε τον υπολογιστή. Τον αφήνουμε ακριβώς όπως είναι, δεν ανοίγουμε αρχεία, δεν εκτελούμε λογισμικό, δεν διαγράφουμε φακέλους, κλπ. Εάν είναι ενεργοποιημένος δεν τον απενεργοποιούμε, και εάν είναι απενεργοποιημένος δεν τον ενεργοποιούμε. Πρέπει να έχουμε κατά νου ότι υπάρχει μεγάλος όγκος μεταβαλλόμενων πληροφοριών (προσωρινής αποθήκευσης), ο οποίος θα διαγραφεί εάν απενεργοποιηθεί ο υπολογιστής. Κατά συνέπεια αν ο υπολογιστής απενεργοποιηθεί, η απενεργοποίηση του θα οδηγούσε στην απώλεια πολύ σημαντικών πληροφοριών. Ομοίως, αν είναι απενεργοποιημένος η ενεργοποίησή του θα μπορούσε να οδηγήσει στην τροποποίηση των ημερομηνιών ή στην απόκρυψη αρχείων αν υπάρχει rootkit.

- Καθιερώνουμε τα γενικά βήματα που πρόκειται να ακολουθηθούν, με στόχο να έχουμε μια συγκεκριμένη κατευθυντήρια γραμμή περιγραφής και εφαρμογής της διαδικασίας συλλογής πληροφοριών και προσέχουμε να μην ξεχνάμε κανέναν βήμα.

- Θα πρέπει να διαθέτουμε μία λεπτομερή περιγραφή των βημάτων της διαδικασίας που πρόκειται να ακολουθήσουμε. Σε αυτό το σημείο, θα πρέπει να λαμβάνονται υπόψη όλες οι πτυχές, όπως ο εκτιμώμενος χρόνος που θα πάρει η ανάλυση, ο επείγων χαρακτήρας της ανάλυσης ή οι αναγκαίοι πόροι για να πραγματοποιηθεί.

- Θα πρέπει να προβλέπουμε και να ελαχιστοποιούμε τους κινδύνους με σκοπό να διασφαλίσουμε, πως στην περίπτωση που θα αυτά προκύψουν προβλήματα δεν θα επηρεάσουν σημαντικά τη διαδικασία με αρνητικό τρόπο.

- Εκτιμούμε εάν το πρόσωπο που είναι υπεύθυνο για τη διεξαγωγή της διαδικασίας έχει την ικανότητα και τις γνώσεις που απαιτούνται για να την πράξει. Αν έχουμε αμφιβολία για την ικανότητά του να την πραγματοποιήσει, το καλύτερο πράγμα που πρέπει να κάνουμε είναι να συμβουλευτούμε κάποιον με εμπειρία και ευρεία γνώση, με σκοπό την παροχή συμβουλών του επί της διαδικασίας με σκοπό την προστασία των δεδομένων και την αποφυγή καταστροφής ή αλλοίωσης αποδεικτικών στοιχείων.

- Θα πρέπει να διαθέτουμε γραπτή άδεια για να είμαστε σε θέση να πραγματοποιήσουμε την ανάλυση και τη συλλογή των αποδεικτικών στοιχείων. Αυτή είναι μια θεμελιώδης αρχή, καθώς εμπιστευτικές πληροφορίες ή ζωτικής σημασίας δεδομένα για μια επιχείρηση θα μπορούσαν να ανακτηθούν κατά την διαδικασία. Θα μπορούσε παράλληλα να επηρεαστεί η διαθεσιμότητα των υπηρεσιών της επιχείρησης από το έργο του εγκληματολογικού ερευνητή. Σε ορισμένα είδη περιστατικών, θα είναι απαραίτητο να ζητηθεί δικαστική άδεια με σκοπό τη διασφάλιση της εγκυρότητας των συγκεντρωθέντων αποδεικτικών στοιχείων σε μια μελλοντική δικαστική υπόθεση.

- Ζητάμε τους απαραίτητους κωδικούς πρόσβασης για να αποκτήσουμε πρόσβαση σε κρυπτογραφημένα αρχεία ή δίσκους (volumes) ή ζητάμε να είναι παρών ο διαχειριστής που κατέχει τους κωδικούς.

- Έχουμε προετοιμάσει μια πλήρη συλλογή εργαλείων για να εφαρμόσουμε όλη την διαδικασία συλλογής αποδεικτικών στοιχείων χωρίς κανένα εμπόδιο.

- Ετοιμάζουμε μια λίστα των ανθρώπων που πρέπει να ενημερώνονται και να διατηρούνται στον κύκλο της διαδικασίας, συμπεριλαμβανομένων του ονόματός τους, της διεύθυνσης ηλεκτρονικού ταχυδρομείου, καθώς και κάθε άλλο είδος πληροφορίας που θα μπορούσε να είναι σχετική.

Η διαδικασία συλλογής αποδεικτικών στοιχείων μπορεί να ξεκινήσει, μόλις έχουμε ξεκαθαρίσει και αξιολογήσει το είδος του κυβερνο-περιστατικού και τα βήματα που πρέπει να ληφθούν για την επίλυσή του.

ΤΜΗΜΑ 16
ΤΑ ΒΑΣΙΚΑ ΓΙΑ ΤΗΝ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΑΝΑΛΥΣΗ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ LINUX

Διεργασίες Linux

Στο λειτουργικό σύστημα Linux, υπάρχουν δύο μέθοδοι για την εκκίνηση μιας διεργασίας - ξεκινώντας την από το προσκήνιο ή το παρασκήνιο. Μπορούμε να ελέγξουμε όλες τις διεργασίες με την εντολή **ps ()** σε ένα παράθυρο τερματικού. Υπάρχουν και άλλα εργαλεία για την προβολή όχι μόνο των διαδικασιών που εκτελούνται στο σύστημα αλλά και την κατανάλωση πόρων (CPU, μνήμη, δίκτυο).

Δύο ευρέως χρησιμοποιούμενα εργαλεία είναι το **top** και το **htop.**

Όπως και στα Windows, αναζητούμε ορφανές (orphan), ζόμπι (zombie) και άλλες ύποπτες διεργασίες στο πλαίσιο της έρευνας μας. Για παράδειγμα αν μια διεργασία εκτελείται με ανοιχτές πόρτες δικτύου, κάτι που δεν συμβαίνει σε παρόμοιο σύστημα, εμπεριέχει κάτι ύποπτο. Μπορεί επίσης να διαπιστώσουμε κορεσμό στο δίκτυο από έναν και μόνο υπολογιστή ή ένα πρόγραμμα που καταναλώνει το 100% της CPU αλλά δεν εμφανίζεται στο σύστημα αρχείων με αυτό το όνομα.

Ext4

Απαραίτητη είναι η εξοικείωση με το σύστημα αρχείων Linux. Το Ext4 είναι ένα από τα πιο δημοφιλή συστήματα αρχείων Linux σήμερα. Έχει πολλές βελτιώσεις σε σχέση με την προκατόχους Ext3 και Ext2. Το Ext4 υποστηρίζει όχι μόνο το **journaling** (περιγράφεται στην επόμενη ενότητα) αλλά και τροποποιεί σημαντικές δομές δεδομένων του συστήματος αρχείων, όπως αυτές που προορίζονται για την αποθήκευση των δεδομένων. Έτσι επιτυγχάνεται βελτίωση της απόδοσης, αξιοπιστία και υποστήριξη πρόσθετων λειτουργιών. Το Ext4 επιτρέπει απεριόριστο αριθμό καταλόγων. Χρησιμοποιεί έναν "multiblock allocator" (mbaloc) για να κατανείμει πολλά μπλοκ σε μία μόνο κλήση, αντί για ένα μεμονωμένο ανά κλήση. Αυτή η δυνατότητα βελτιώνει δραστικά την απόδοση του συστήματος.
Πριν ξεκινήσουμε την διαδικασία της ανάλυσης καλό είναι να αποκτήσουμε οικειότητα με το σύστημα αρχείων έτσι ώστε να είμαστε σε θέση να αντιληφθούμε περίεργες συμπεριφορές. Για παράδειγμα σε ένα παραβιασμένο σύστημα, μπορεί ένα διαμέρισμα (partition) να εμφανίζει 100% χρήση, αλλά με την εντολή **du**, το σύστημα μπορεί να παρουσιάσει ότι χρησιμοποιείται μόνο κατά 30%.
Τα δύο δημοφιλέστερα εργαλεία για την ανάλυση του συστήματος αρχείων σε περιβάλλον Linux είναι το Sleuth Kit και το Autopsy[5].

Journaling

Τα Ext4 και Ext3 είναι συστήματα αρχείων τύπου journaling. Ένα τέτοιο σύστημα διατηρεί την καταγραφή των αλλαγών που δεν έχουν ακόμη αποδοθεί στο κύριο μέρος. Αυτή η δομή δεδομένων αναφέρεται ως "journal", το οποίο είναι ένα κυκλικό αρχείο καταγραφής με κύριο χαρακτηριστικό την πολύ γρήγορη αποκατάσταση σε περίπτωση κατάρρευσης (crash) ή διακοπής της τροφοδοσίας. Το journaling εξασφαλίζει την ακεραιότητα (integrity) του συστήματος αρχείων παρακολουθώντας όλες τις αλλαγές στο δίσκο, με μία μικρή αύξηση στην κατανάλωση πόρων.

Το Master Boot Record στο Linux και το Συστήμα Αρχείων Swap

Το MBR (Master Boot Record) είναι ένας ειδικός τομέας εκκίνησης (boot sector) που περιέχει 512 ή περισσότερα bytes στον πρώτο τομέα της μονάδας δίσκου. Το MBR περιλαμβάνει οδηγίες σχετικά με τον τρόπο αρχειοθέτησης των λογικών διαμερισμάτων (logical partitions) στη μονάδα δίσκου. Έχει επίσης εκτελέσιμο

[5] Και τα δύο εργαλεία βρίσκονται στον ιστότοπο https://www.sleuthkit.org/

κώδικα για να φορτώσει το λειτουργικό σύστημα. Οι πιο συνηθισμένοι boot loaders στο Linux είναι ο Linux Loader (LILO), το Load Linux (LOADLIN) και ο Grand Unified Bootloader (GRUB). Υπάρχουν δύο κύρια διαμερίσματα (partitions) σε ένα σύστημα Linux: το διαμέρισμα δεδομένων (data partition), το οποίο περιέχει όλα τα δεδομένα του συστήματος Linux μαζί με το διαμέρισμα root και το διαμέρισμα swap, το οποίο είναι επιπλέον μνήμη στη μονάδα σκληρού δίσκου ως επέκταση της φυσικής μνήμης του συστήματος.
Ο χώρος swap είναι προσβάσιμος και ορατός μόνο από το ίδιο το σύστημα. Το swap εξασφαλίζει ότι το λειτουργικό σύστημα συνεχίζει να λειτουργεί. Τα Windows, το Mac OS X και άλλα λειτουργικά συστήματα χρησιμοποιούν επίσης swap ή εικονική μνήμη. Ο χώρος swap είναι πιο αργός από την πραγματική φυσική μνήμη RAM, αλλά βοηθά εξαιρετικά στη λειτουργία του συστήματος. Ένας γενικός κανόνας είναι ότι το Linux συνήθως έχει διπλάσια swap από τη φυσική μνήμη.
Ένα ενδιαφέρον σημείο είναι ότι οτιδήποτε στη μνήμη RAM έχει τη δυνατότητα να αποθηκεύεται στον χώρο swap ανά πάσα στιγμή. Εκεί μπορούμε να βρούμε δεδομένα χωρίς κρυπτογράφηση, κλειδιά κρυπτογράφησης, διαπιστευτήρια χρηστών, μηνύματα ηλεκτρονικού ταχυδρομείου και άλλες ευαίσθητες πληροφορίες.

ΤΜΗΜΑ 17
ΕΝΑΡΞΗ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ

Η πρωταρχική ενέργεια μας είναι να κάνουμε καταγραφή-απογραφή (tag) του υλικού. Καταγράφουμε και φωτογραφίζουμε κάθε συσκευή που πρόκειται να αναλυθεί: σκληρούς δίσκους, pen drives, φωτογραφικές μηχανές, κλπ. Επίσης, ανάλογα με το είδος του περιστατικού, μπορεί να είναι απαραίτητο να συμπεριλάβουμε δρομολογητές, σαρωτές, εκτυπωτές, κλπ. Πρέπει να σημειωθούν, από όλα, η μάρκα, το μοντέλο, ο σειριακός αριθμός, ο τύπος της σύνδεσης (USB, firewire, κλπ). Ομοίως, θα πρέπει να καταγραφούν οι πληροφορίες του προσώπου που είναι υπεύθυνο για το σύστημα και ο χρήστης ή οι χρήστες που εργάζονται σε αυτό, καθώς και κάθε άλλη σχετική πληροφορία θα πρέπει να καταγραφεί. Θα πρέπει να σημειωθεί και το όνομα του χρήστη που εργαζόταν στο συγκεκριμένο σύστημα όταν καταγράφτηκε το γεγονός/περιστατικό. Η αλυσίδα της παρακολούθησης/επιμέλειας είναι θεμελιώδης, διότι αποδεικνύει ότι τα ληφθέντα αποδεικτικά στοιχεία δεν έχουν παραποιηθεί. Είναι υποχρεωτική η ιδιαίτερη σχολαστικότητα με την οποία διαχειριζόμαστε τα δεδομένα που συλλέγουμε. Για να γίνει αυτό, είναι απαραίτητο να καταγράψουμε όλα τα αποδεικτικά στοιχεία που ελήφθησαν.

Στις παρατηρήσεις, είναι σημαντικό να δικαιολογήσουμε το λόγο ως προς το γιατί τα προαναφερθέντα αποδεικτικά στοιχεία έχουν συλλεχθεί. Ο στόχος αυτού του βήματος είναι να διευκολύνει το έργο του αναλυτή, αν ο ίδιος ο ερευνητής δεν είναι το πρόσωπο που εκτελεί το ρόλο αυτό.

Από τη στιγμή που όλες οι συσκευές έχουν καταγραφεί, απογραφεί και φωτογραφηθεί, τα αποδεικτικά στοιχεία μπορούν να αρχίσουν να συγκεντρώνονται. Κατά ένα γενικό τρόπο, το είδος των αποκτηθέντων πληροφοριών μπορούν να ταξινομηθούν σε δύο μεγάλες ομάδες: μεταβλητές /

πτητικές πληροφορίες (προσωρινής αποθήκευσης) και μη-μεταβλητές πληροφορίες (μόνιμης αποθήκευσης). Μπορούμε επίσης να μιλήσουμε για ζωντανή-ενεργή απόκτηση πληροφοριών που αντιστοιχεί στη συγκέντρωση των πληροφοριών σε ένα σύστημα που λειτουργεί, καθώς και για στατική απόκτηση πληροφοριών που αντιστοιχεί στη συγκέντρωση των πληροφοριών σε ένα σύστημα που είναι απενεργοποιημένο.

Σημαντικό

Για να πραγματοποιήσουμε μια σωστή συλλογή αποδεικτικών στοιχείων, είναι σημαντικό να χρησιμοποιήσουμε "καθαρό" μη μολυσμένο λογισμικό που μπορεί να το έχουμε σε συσκευές που προστατεύονται από την εγγραφή (pen drive, CD-ROM, κλπ.). Ομοίως, αν υπάρχει υποψία ότι το σύστημα έχει παραβιαστεί/προσβληθεί από ιομορφικό λογισμικό, τότε οι πληροφορίες πρέπει να συλλέγονται με την χρήση στατικών εκτελέσιμων αρχείων και όχι με την χρήση των APIs του συστήματος, διότι η ακεραιότητα των τελευταίων ενδέχεται να έχει αλλοιωθεί και δεν θα παρουσιάζουν τα πραγματικά αποτελέσματα.

Στην συνέχεια παρουσιάζονται μια σειρά από ελεύθερα λογισμικά και live CDs που μπορούν να χρησιμοποιηθούν δωρεάν κατά την διαδικασία της ψηφιακής εγκληματολογικής ανάλυσης. Ωστόσο ανάλογα με την εμπειρία του ερευνητή, μπορεί ο ίδιος να δημιουργήσει μία αντίστοιχη εργαλειοθήκη σύμφωνα με τις ανάγκες του.

Όνομα	*URL*
SIFT	*SANS Investigative Forensic Toolkit (SIFT) http://digital-forensics.sans.org/community/downloads*
Caine	*http://www.caine-live.net*
Digital Forensics Framework	*http://www.digital-forensic.org*
The Sleuth Kit y AutoSpy	*http://www.sleuthkit.org*
Helix Live CD	*http://www.e-fense.com*

Πίνακας 1: Λίστα από open source συλλογές εργαλείων για την ψηφιακή εγκληματολογική ανάλυση.

Σημείωση

Συνήθως, είναι δυνατό να λαμβάνουμε μόνο ένα αντίγραφο της μνήμης (memory dump) και μόνο ένα αντίγραφο του δίσκου (disk dump), και από εκεί να εργαζόμαστε σε διαφορετικά αντίγραφα για να αποκτήσουμε το υπόλοιπο των αποδεικτικών στοιχείων. Η συλλογή πληροφοριών εξαρτάται από την υπόθεση και ανάλογα με την περίπτωση, μπορεί να μην είναι απαραίτητο να πραγματοποιήσουμε έναν ολικό αντίγραφο του συνόλου των πληροφοριών, αλλά μια απλή συλλογή συγκεκριμένων πληροφοριών να μας βοηθήσουν να επιλύσουμε την υπόθεση.

ΤΜΗΜΑ 18
ΜΕΤΑΒΛΗΤΕΣ (ΠΡΟΣΩΡΙΝΗΣ ΑΠΟΘΗΚΕΥΣΗΣ) ΠΛΗΡΟΦΟΡΙΕΣ

Οι μεταβλητές - πτητικές πληροφορίες (προσωρινής αποθήκευσης), είναι πολύ σημαντικές κατά την εκτέλεση της ψηφιακής εγκληματολογικής ανάλυσης, διότι ενδέχεται να περιέχουν αποδεικτικά στοιχεία συνδέσεων, διεργασιών, υπηρεσιών, κλπ. Η απώλεια αυτού του είδους των πληροφοριών θα μπορούσε να σημαίνει ότι η ψηφιακή εγκληματολογική ανάλυση δεν έχει ολοκληρωθεί με επιτυχία ή ότι η διαδικασία θα γίνει περίπλοκη σε μεγάλο βαθμό, διότι θα λείπουν δεδομένα. Παρακάτω υποδεικνύεται η μέθοδος που πρέπει να χρησιμοποιείται, και παρουσιάζονται μερικά παραδείγματα περιστατικών όπου θα μπορούσαν να είναι χρήσιμα. Με αυτόν τον τρόπο, ο υπεύθυνος που πραγματοποιεί τη διαδικασία, μπορεί να συμπληρώσει τα βήματα που θεωρεί κατάλληλα, χρησιμοποιώντας τις κατευθυντήριες οδηγίες που δίνονται εδώ ως βάση. Η σειρά των ενεργειών είναι η παρακάτω :

- Ανάκτηση Αντιγράφου Φυσικής Μνήμης (Physical Memory) και ανάλυση του
- Καταγραφή Λεπτομερειών Συστήματος
- Συνδεδεμένοι Χρήστες στο Σύστημα
- Συνδέσεις και Δραστηριότητα Δικτύου
- Τρέχουσες Διεργασίες
- Συσχέτιση Θυρών και Διεργασιών
- Εντοπισμός Ύποπτων Υπηρεσιών
- Ανάκτηση Ενοτήτων Πυρήνα (Kernel Modules)
- Εντοπισμός ανοικτών αρχείων
- Ανάκτηση Ιστορικού Εντολών
- Επιθεώρηση Κοινοχρήστων Δικτύου (Network Shares)
- Εξέταση Προγραμματισμένων Εργασιών
- Εξέταση Περιεχομένων Πρόχειρου (Clipboard)
- Εντοπισμός των αρχείων setuid και setgid

- **<u>Ανάκτηση Αντιγράφου Φυσικής Μνήμης (Physical Memory)</u>**

Η ανάκτηση αντιγράφου φυσικής μνήμης είναι μία από τις πιο σημαντικές και κρίσιμες ενέργειες στη φάση συλλογής των πληροφοριών. Όπως αναφέρθηκε προηγουμένως, η μνήμη αποθηκεύει σημαντικά αποδεικτικά στοιχεία, όπως εγκατεστημένες συνδέσεις, εκτελούμενες διεργασίες/υπηρεσίες, κρυπτογραφημένα συνθηματικά (passwords), κλπ. Η λήψη ενός σωστού αντιγράφου μνήμης μπορεί να κάνει τη διαφορά μεταξύ της επίλυσης ή της μη επίλυσης ενός κυβερνο-περιστατικού. Εξαιτίας αυτού πρέπει να είμαστε πολύ προσεκτικοί κατά τη διάρκεια αυτής της διαδικασίας συλλογής της μνήμης.

Η συλλογή της μνήμης είναι πολύ σημαντική πριν από οποιαδήποτε άλλη ενέργεια διότι η διαδικασία της συλλογής των πτητικών δεδομένων, θα μεταβάλλει τα περιεχόμενα στο υπό εξέταση σύστημα.

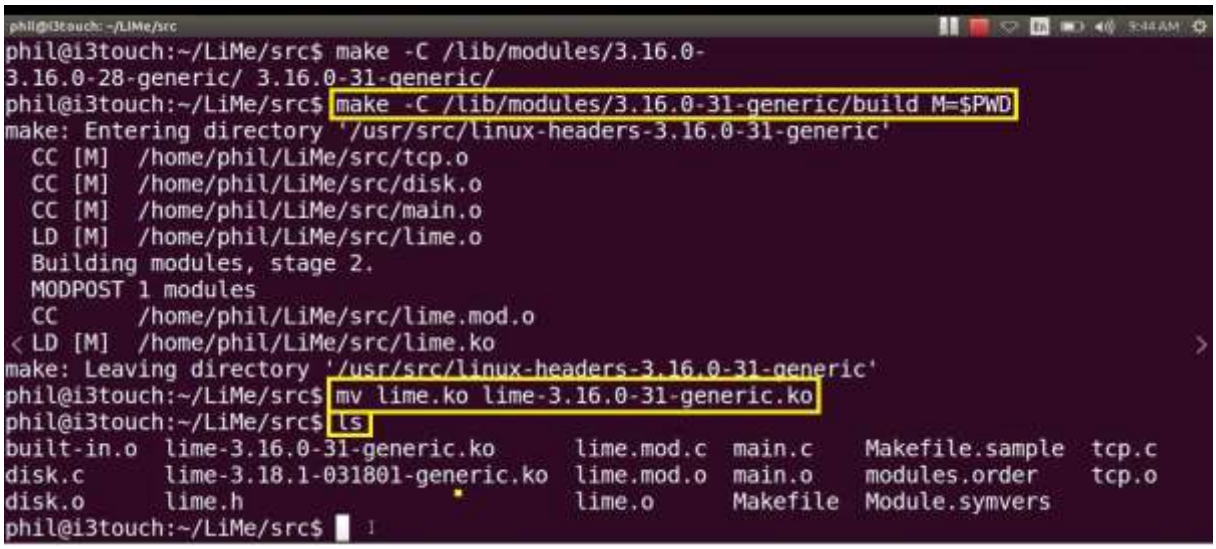
Υπάρχει αριθμός εργαλείων που επιτρέπουν την λήψη αντιγράφου μνήμης, με τα δύο δημοφιλέστερα να είναι το **LiME** και το **fmem**.

Εργαλεία

LiME	https://github.com/504ensicsLabs/LiME
fmem	http://hysteria.sk/~niekt0/fmem/fmem_current.tgz

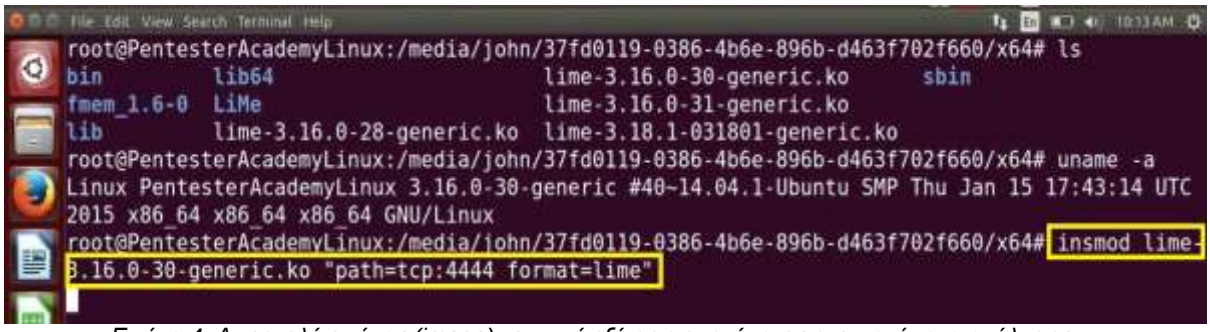
Lime

Το **LiME** (Linux Memory Extractor) είναι ένα άρθρωμα πυρήνα (kernel module) για την ανάκτηση των δεδομένων της φυσικής μνήμης σε συστήματα Linux και Android. Η ανάκτηση μπορεί να γίνει σε τοπικό αποθηκευτικό μέσο (συσκευή USB ή κάρτα SD) ή μέσω του δικτύου. Η διαδικασία της ανάκτησης μνήμης πρέπει να γίνει με συγκεκριμένη διαδικασία. Αρχικά το άρθρωμα πρέπει να δημιουργηθεί (build) στην ίδια ακριβώς έκδοση πυρήνα με αυτήν του υπό εξέταση συστήματος, σε ένα σύστημα διαφορετικό από το υπό εξέταση[6]. .Ένα παράδειγμα για την δημιουργία του module φαίνεται στην Εικόνα 3: Όταν στήσουμε αυτό το σύστημα με την ίδια έκδοση πυρήνα δίνουμε την εντολή **sudo apt-get install lime-forensics-dkms** στο μηχάνημα ανάλυσης. Ακολούθως, αντιγράφω τα modules του lime στη συσκευή USB που θα χρησιμοποιήσω για την ανάκτηση της μνήμης. Μετά εισάγω στο υπό εξέταση μηχάνημα τη συσκευή USB. Επιλέγω την διαμόρφωση (format) του παραγόμενου αρχείου με τις επιλογές raw, padded, lime. Η εντολή για την ανάκτηση και αποστολή της μνήμης στο μηχάνημα ανάλυσης είναι της μορφής: **sudo insmod lime.ko "path=tcp:4444 format=lime"** (Εικόνα 4)



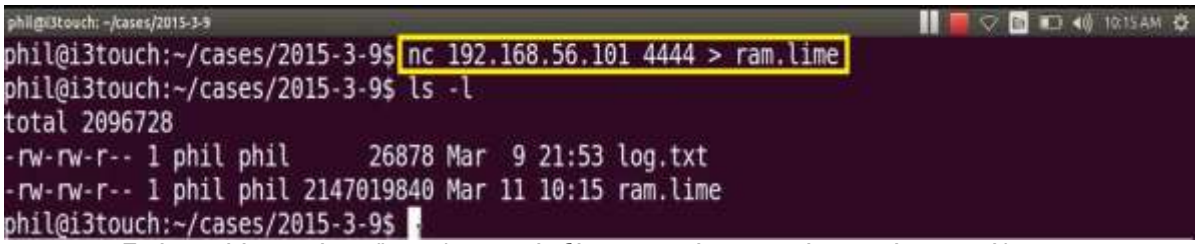
Εικόνα 3: make του προγράμματος LiME στο μηχάνημα ανάλυσης

[6] Η σύγκριση των εκδόσεων του πυρήνα γίνεται με την εκτέλεση της εντολής uname – a και στα δυο μηχανήματα και την σύγκριση των αποτελεσμάτων μεταξύ τους



Εικόνα 4: Αποστολή εικόνας (image) του υπό εξέταση συστήματος στο μηχάνημα ανάλυσης

Και ανοίγουμε το netcat στο μηχάνημα ανάλυσης για την λήψη της εικόνας (image)



Εικόνα 5:Λήψη εικόνας (image) του υπό εξέταση συστήματος από το μηχάνημα ανάλυσης

Αυτό που προκύπτει τελικά είναι ένα αρχείο της μορφής ram.lime το οποίο θα αναλύσουμε με το εργαλείο volatility[7].

fmem

Το **fmem** (forensics memory) είναι επίσης ένα άρθρωμα πυρήνα (kernel module) για την λήψη αντιγράφου της μνήμης. Ουσιαστικά δημιουργεί μία ψευδοσυσκευή (pseudo-device) στην τοποθεσία /dev/fmem, παρόμοια με την /dev/mem η οποία ακολούθως μπορεί να αντιγραφεί με εργαλεία όπως το dd. Ομοίως και εδώ όπως με το LiME ποτέ δεν κάνουμε build το λογισμικό στο υπό εξέταση σύστημα, αλλά σε ένα ίδιο ακριβώς είτε φυσικά είτε σε εικονικό περιβάλλον (virtual machine). Αφού γίνει build τότε χρησιμοποιούμε το αρχείο /proc/iomem για να καθορίσουμε ποια σημεία της μνήμης μας ενδιαφέρουν. Το μειονέκτημα της παραπάνω διαδικασίας είναι ότι δεν παράγεται κάποια εικόνα της μνήμης (image) έτσι ώστε να χρησιμοποιηθεί από εργαλεία που θα διευκολύνουν το έργο της ανάλυσης όπως το volatility.
Η εντολή που δίνουμε είναι η ακόλουθη:

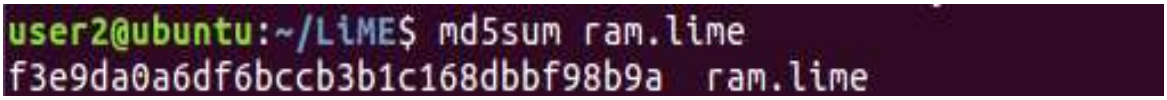
$ dcfldd if=/dev/fmem of=memory.dump hash=sha256 sha256log=memory.dump.sha256 bs=1MB count=1000

Σημαντικό

Μόλις ληφθεί το αντίγραφο (image) της μνήμης, είναι απαραίτητο να πραγματοποιήσουμε και τον έλεγχο ακεραιότητας του συγκεκριμένου αρχείου

[7] Η διαδικασία περιγράφεται με απλά βήματα και στον παρακάτω σύνδεσμο https://www.youtube.com/watch?v=_7Tq8dcmP0k

(τμήμα 21). Στο πλαίσιο της διαδικασία επιτήρησης, καταγράφουμε τις τιμές του ελέγχου ακεραιότητας (σωστό είναι να το κάνουμε και με διαφορετικούς αλγορίθμους). Σκοπός μας είναι να τηρήσουμε την διαδικασία επιτήρησης-παρακολούθησης και να εγγυηθούμε ότι το προαναφερθέν αντίγραφο (image) δεν έχει τροποποιηθεί μεταγενέστερα.(Εικόνα)



Εικόνα 6 Ένα απλό πρόγραμμα ελέγχου ακεραιότητας

Αφού γίνει και αυτή η ενέργεια τότε μπορούμε να απενεργοποιήσουμε το υπό εξέταση σύστημα επιλέγοντας την καλύτερη μέθοδο. Οι επιλογές που έχουμε είναι δύο, η κανονική απενεργοποίηση ή η απότομη διακοπή της τροφοδοσίας του ρεύματος. Η πρώτη μέθοδος θα επιτρέψει στο σύστημα αρχείων να κλείσει κανονικά όμως το ιομορφικό λογισμικό ενδέχεται να καταστρέψει κάποια αποδεικτικά στοιχεία. Η δεύτερη μέθοδος θα μας αφήσει με ένα σύστημα αρχείων που δεν θα είναι καθαρό (πχ. η cache μνήμη δεν θα έχει γίνει flash), όμως το ιομορφικό λογισμικό δεν θα μπορέσει να επιφέρει καμία αλλαγή στο σύστημα αλλοιώνοντας αποδεικτικά στοιχεία.

Ανάλυση Αντιγράφου Φυσικής Μνήμης (Physical Memory)

Η επόμενη ενέργεια αφού κάνουμε ανάκτηση της μνήμης είναι να εκκινήσουμε την διαδικασία ανάλυσης της. Αυτή η διαδικασία προτείνεται να γίνει με το εργαλείο volatility. Το volatility είναι γραμμένο στην γλώσσα προγραμματισμού python και αρχικά είχε αναπτυχθεί για την εξέταση ιμνήμης σε περιβάλλον Windows. Η έκδοση σε περιβάλλον Linux χρησιμοποιείται για την εξαγωγή πληροφοριών σχετικά με διεργασίες, συνδέσεις δικτύου, ανοικτά handles και πολλές άλλες πληροφορίες του συστήματος. Αναλυτικές οδηγίες για την εγκατάσταση του, υπάρχουν στον ιστότοπο

https://github.com/volatilityfoundation/volatility/wiki/Installation

Αφού γίνει η εγκατάσταση του προγράμματος και πριν την διαδικασία εκκίνησης της ανάλυσης, θα πρέπει να δημιουργήσουμε το profile του συγκεκριμένου υπό εξέταση λειτουργικού. Η μεθοδολογία αναλύεται με απλά βήματα στον ιστότοπο

https://github.com/volatilityfoundation/volatility/wiki/Linux

Περιληπτικά, πρέπει να προηγηθεί η εγκατάσταση των εργαλείων dwarfdump, GCC/make και των headers για την δημιουργία των αρθρωμάτων του πυρήνα (kernel modules). Στην περίπτωση των Debian/Ubuntu δίνουμε τις εντολές:

$ sudo apt-get install dwarfdump
$ apt-get install build-essential
$ apt-get install linux-headers-$(uname -r)[8]

[8] Η εντολή uname –r επιστρέφει την έκδοση του πυρήνα την οποία χρησιμοποιώ για την

Επόμενο βήμα είναι να δώσουμε την εντολή make στον φάκελο volatility/tools/linux, εντολές:

$ cd volatility/tools/linux
 # make

```
root@ubuntu:/usr/src/volatility-tools/linux# make
make -C //lib/modules/4.10.0-28-generic/build CONFIG_DEBUG_INFO=y M="/usr/src/vo
latility-tools/linux" modules
make[1]: Entering directory '/usr/src/linux-headers-4.10.0-28-generic'
  CC [M]  /usr/src/volatility-tools/linux/module.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /usr/src/volatility-tools/linux/module.mod.o
  LD [M]  /usr/src/volatility-tools/linux/module.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.10.0-28-generic'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/4.10.0-28-generic/build M="/usr/src/volatility-tools/linux
" clean
make[1]: Entering directory '/usr/src/linux-headers-4.10.0-28-generic'
  CLEAN   /usr/src/volatility-tools/linux/.tmp_versions
  CLEAN   /usr/src/volatility-tools/linux/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-4.10.0-28-generic'
root@ubuntu:/usr/src/volatility-tools/linux#
```

Το αρχείο που παράγεται είναι της μορφής module.dwarf. Ακολούθως δημιουργώ ένα αντίγραφο το αρχείου System.map και του δίνω δικαιώματα ανάγνωσης-εγγραφής.

 # cp System.map-4.10.0-28-generic System.map-4.10.0-28-generic-copy
 # chmod 644 System.map-4.10.0-28-generic-copy

```
root@ubuntu:/boot# cp System.map-4.10.0-28-generic System.map-4.10.0-28-generic-
copy
root@ubuntu:/boot# ls
abi-4.10.0-28-generic         memtest86+.elf
config-4.10.0-28-generic      memtest86+_multiboot.bin
grub                          System.map-4.10.0-28-generic
initrd.img-4.10.0-28-generic  System.map-4.10.0-28-generic-copy
memtest86+.bin                vmlinuz-4.10.0-28-generic
root@ubuntu:/boot# chmod 644 System.map-4.10.0-28-generic-copy
root@ubuntu:/boot#
```

Η επόμενη ενέργεια είναι να ετοιμάσουμε ένα zip αρχείο που θα περιέχει το module.dwarf και το system.map με την εντολή:

 # zip Ubuntu1604.zip volatility/tools/linux/module.dwarf /boot/System.map-4.10.0-28-generic-copy

Με αυτό τον τρόπο έχουμε ετοιμάσει το Ubuntu profile για το υπό εξέταση σύστημα

εγκατάσταση των headers.

```
root@ubuntu:/usr/share/volatility# zip Ubuntu1604.zip tools/linux/module.dwarf /
boot/System.map-4.10.0-28-generic-copy
  adding: tools/linux/module.dwarf (deflated 89%)
  adding: boot/System.map-4.10.0-28-generic-copy (deflated 79%)
root@ubuntu:/usr/share/volatility#
```

Και ακολούθως θα το αντιγράψουμε στον αντίστοιχο φάκελο του προγράμματος που περιέχει τα profiles

```
root@ubuntu:/usr/share/volatility# cp Ubuntu1604.zip /usr/lib/python2.7/dist-pac
kages/volatility/plugins/overlays/linux
root@ubuntu:/usr/share/volatility#
```

Για να δούμε τα ububtu profiles που έχουμε αποθηκευμένα, δίνουμε την εντολή:

python vol.py --info | grep Ubuntu

```
root@ubuntu:/usr/share/volatility# python vol.py --info | grep Ubuntu
Volatility Foundation Volatility Framework 2.5
LinuxUbuntu1604x64 - A Profile for Linux Ubuntu1604 x64
root@ubuntu:/usr/share/volatility#
```

Οι εντολές που εκτελούμε για την ανάκτηση των πληροφοριών που θέλουμε περιγράφονται στον ιστότοπο

https://github.com/volatilityfoundation/volatility/wiki/Volatility-Usage

Οι βασικές εντολές του Volatility είναι όπως παρακάτω. Αντικαθιστούμε το όνομα του plugin με αυτό που θέλουμε να χρησιμοποιήσουμε, το path που υπάρχει το image της μνήμης και το όνομα του profile με αυτό που έχουμε δημιουργήσει.

$ python vol.py [plugin] -f [image] --profile=[profile]

Ένα παράδειγμα είναι το παρακάτω:
$ python vol.py linux_pslist -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64

Μερικά παραδείγματα εντολών για την αποτελεσματικότερη χρήση του εργαλείου είναι οι εξής:

$ python vol.py linux_pslist_cache -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (περιλαμβάνει εισαγωγές διεργασιών που παρέχουν λίστα με ενεργές, τερματισμένες και κρυφές διεργασίες)
$ python vol.py linux_kmem_cache -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (μία διαφορετική προσέγγιση για να βρούμε κρυφές διεργασίες από τις λεπτομέρειες της kmem_cache)
$ python vol.py linux_psaux -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (περιλαμβάνει λεπτομέρειες για τρέχουσες διεργασίες)
$ python vol.py linux_psxview -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (συγκρίνει το αποτέλεσμα διάφορων διεργασιών με

σκοπό την αποκάλυψη ασυμφωνιών που προκαλεί η παρουσία ιομορφικού λογισμικού)
$ python vol.py linux_lsmod -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (παρέχει λίστα με τα αρθρώματα (modules) που τρέχουν στο σύστημα)
$ python vol.py linux_check_modules -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (βρίσκει ασυμφωνίες μεταξύ της λίστας των αρθρωμάτων (modules) και των πληροφοριών κάτω από /sys/modules για την αποκάλυψη κρυφών αρθρωμάτων)
$ python vol.py linux_proc_maps -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (παρέχει μία λίστα με τις βιβλιοθήκες για κάθε διεργασία μαζί με τις περιοχές της μνήμης που έχουν δεσμευτεί για την κάθε διεργασία)
$ python vol.py linux_dump_map -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (αποθηκεύει (dump) συγκεκριμένες βιβλιοθήκες και περιοχές της μνήμης για την εκτέλεση σε βάθος ανάλυση)
$ python vol.py linux_lsof -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (δείχνει τα αρχεία στα οποία έχει πρόσβαση κάθε διεργασία)
$ python vol.py linux_find_file -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (εξάγει από τη μνήμη για περαιτέρω εξέταση ένα αρχείο που ενδέχεται να χρησιμοποιείται από το ιομορφικό λογισμικό για την συλλογή ονομάτων χρηστών, συνθηματικών και κίνησης δικτύου)
$ python vol.py linux_netstat -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (εξάγει τις ανοικτές θύρες ή ενεργές συνδέσεις δικτύου από τη μνήμη που έχουν συσχετισθεί με κάποια διεργασία ενδιαφέροντος)
$ python vol.py linux_dmesg -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (εξάγει πληροφορίες συστήματος και αρχεία καταγραφής)
$ python vol.py linux_tmpfs -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (εξάγει τα προσωρινά αρχεία συστήματος που έχουν φορτωθεί (mounted) στη μνήμη)
$ python vol.py linux_bash -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (εξάγει την ακολουθία των εντολών που έχουν εκτελεστεί από τη μνήμη)
$ python vol.py linux_check_syscall -f /home/lab/memory.lime --profile=LinuxUbuntu1604x64 (ανιχνεύει αλλοιώσεις στη λίστα κλήσεων του συστήματος (system call table))

Καταγραφή Λεπτομερειών Συστήματος

Αφού έχουμε αποκτήσει την εικόνα (image) της μνήμης από το σύστημα, ξεκινάμε την συλλογή δεδομένων από το υπό εξέταση σύστημα από την ημερομηνία και την ώρα. Αυτή η ενέργεια αποτελεί την βάση για την έρευνα μας καθώς και την αναφορά που θα συντάξουμε. Προηγουμένως όμως με την εντολή script καταγράφουμε όλες τις εντολές που θα δώσουμε στο σύστημα για την συγκέντρωση των πτητικών δεδομένων.

```
user2@ubuntu:~$ script
Script started, file is typescript
user2@ubuntu:~$
```

Ακολούθως μία στατική έκδοση (statically compiled) της εντολής date η οποία απεικονίζει τις παρακάτω πληροφορίες:

```
user2@ubuntu:~$ date
Tue Oct  3 14:17:22 PDT 2017
user2@ubuntu:~$
```

Εκτός από την ημερομηνία και την ώρα του συστήματος, συγκεντρώνουμε πληροφορίες που αφορούν φυσικά χαρακτηριστικά όπως αύξων αριθμός (serial number), μάρκα, μοντέλο και τυχόν άλλα φυσικά χαρακτηριστικά που το προσδιορίζουν με μοναδικό τρόπο. Αυτό γίνεται με την εντολή dmidecode.

 # dmidecode –t system | grep Serial

```
user2@ubuntu:~$ sudo dmidecode -t system | grep Serial
        Serial Number: VMware-56 4d cb a0 9a 2f aa 49-dd 1b 9d 5b 59 9a 71 85
```

<u>Συνδεδεμένοι Χρήστες στο Σύστημα</u>

Ακολούθως συγκεντρώνουμε τα ονόματα χρηστών με τις παρακάτω εντολές :

$ whoami
$ id
$ logname

```
root@ubuntu:~# whoami
root
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# logname
lab
root@ubuntu:~#
```

<u>Συνδέσεις και Δραστηριότητα Δικτύου</u>

Όταν καταγράφουμε τις ρυθμίσεις του συστήματος προσέχουμε για οποιοδήποτε ύποπτο χαρακτηριστικό. Εντοπίζουμε αν υπάρχουν εικονικά ιδιωτικά δίκτυα (Virtual

Private Network -VPN) ενεργοποιημένα στον υπολογιστή και ελέγχουμε αν κάποια από τις κάρτες δικτύου είναι σε promiscuous mode κάτι που υποδηλώνει την ύπαρξη ενός sniffer[9]. Η εντολή που χρησιμοποιούμε είναι η ifconfig.

$ ifconfig -a

```
root@ubuntu:/home/user2# ifconfig -a
ens33     Link encap:Ethernet  HWaddr 00:0c:29:9a:71:85
          inet addr:192.168.110.131  Bcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::7168:3f20:50ae:6d01/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:418 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12284 (12.2 KB)  TX bytes:39835 (39.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:488 errors:0 dropped:0 overruns:0 frame:0
          TX packets:488 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34612 (34.6 KB)  TX bytes:34612 (34.6 KB)
```

Με την παρακάτω εντολή ελέγχω εάν κάποια συσκευή δικτύου είναι σε promiscuous mode

$ tail -f /var/log/syslog

```
root@ubuntu:~# tail -f /var/log/syslog
Jun 10 00:00:01 ubuntu CRON[3217]: (root) CMD (   test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.5min ))
Jun 10 00:00:01 ubuntu CRON[3218]: (root) CMD (/etc/cron.5min/dpkg)
Jun 10 00:00:01 ubuntu CRON[3219]: (root) CMD (   test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.5min ))
Jun 10 00:02:50 ubuntu kernel: [ 1585.574584] Netfilter messages via NETLINK v0.30.
Jun 10 00:02:50 ubuntu kernel: [ 1585.575151] type=1400 audit(1465542167.883:65): apparmor="DENIED" operation="capable" profile="/usr
" pid=3225 comm="tcpdump" capability=12  capname="net_admin"
Jun 10 00:02:50 ubuntu kernel: [ 1585.575251] device eth0 entered promiscuous mode
Jun 10 00:04:12 ubuntu kernel: [ 1670.278507] device eth0 left promiscuous mode
Jun 10 00:04:30 ubuntu kernel: [ 1688.345623] device eth0 entered promiscuous mode
Jun 10 00:05:39 ubuntu kernel: [ 1757.395000] device eth0 left promiscuous mode
Jun 10 00:06:02 ubuntu kernel: [ 1780.719686] device eth0 entered promiscuous mode
```

Με την παρακάτω εντολή ελέγχω τον χρόνο λειτουργίας του υπό εξέταση συστήματος από την τελευταία επανεκκίνηση και το πόσο απασχολημένος ήταν βοηθώντας στην εξέταση των τρεχουσών διεργασιών.

$ uptime

[9] Σε αυτόν τον ιστότοπο https://www.lifewire.com/definition-of-sniffer-817996 περιγράφεται η λειτουργία ενός sniffer δικτύου

```
root@ubuntu:/home/user2# uptime
 14:23:41 up 8 min,  1 user,  load average: 0.02, 0.28, 0.22
```

Με την εντολή uname συγκεντρώνουμε μια σειρά δεδομένων που αφορούν τις μεταβλητές περιβάλλοντος του συστήματος που θα αποκαλύψουν μη αναβαθμισμένα προγράμματα, ευάλωτα σε επιθέσεις:

$ uname –a

```
root@ubuntu:/home/user2# uname -a
Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 20
17 x86_64 x86_64 x86_64 GNU/Linux
```

Μια λεπτομερής εικόνα του συστήματος σχετικά με τις παραπάνω πληροφορίες παίρνουμε με την εντολή printenv[10]

$ printenv

```
root@ubuntu:/home/user2# printenv
SHELL=/bin/bash
TERM=xterm-256color
USER=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd
=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;4
4:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;
31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7
z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=0
1;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz
=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*
.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;3
1:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm
=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:
*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=0
1;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*
.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;
35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=
01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.o
gv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36
:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=0
0;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
SUDO_USER=user2
SUDO_UID=1000
USERNAME=root
MAIL=/var/mail/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games
PWD=/home/user2
LANG=en_US.UTF-8
SHLVL=1
SUDO_COMMAND=/bin/su
HOME=/root
```

Επιπρόσθετες πληροφορίες όπως η έκδοση του compiler είναι διαθέσιμες στο αρχείο /proc/version

[10] Η εντολή printenv εκτυπώνει τα ονόματα και τις τιμές όλων των μεταβλητών περιβάλλοντος του συστήματος

```
root@ubuntu:/home/user2# cat /proc/version
Linux version 4.10.0-28-generic (buildd@lgw01-12) (gcc version 5.4.0 20160609 (U
buntu 5.4.0-6ubuntu1~16.04.4) ) #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2
017
```

Η εντολή sa δίνει μία σύνοψη των εντολών που έχουν εκτελεστεί στο σύστημα

$ sa

```
user2@ubuntu:~$ sa
     61       0.35re       0.04cp        0avio      6985k
     34       0.30re       0.04cp        0avio      6879k   ***other*
      3       0.00re       0.00cp        0avio     10847k   perl
     13       0.01re       0.00cp        0avio      6599k   dpkg
      5       0.00re       0.00cp        0avio     10510k   apt-config
      4       0.03re       0.00cp        0avio      1127k   sh
      2       0.00re       0.00cp        0avio      8409k   systemctl
```

Εάν έχουμε εγκαταστήσει το System Activity Reporter (sar), τότε η εντολή sar παρέχει διάφορες λεπτομέρειες σχετικά με τη χρήση της CPU, των I/O, τις συσκευές μνήμης, και το δίκτυο κατά συγκεκριμένο χρονικό διάστημα (προεπιλογή είναι καθημερινές αναφορές με διαλείμματα 10 λεπτών). Τα αποτελέσματα των αναφορών από το SAR αποθηκεύονται στο directory /var/log/sysstat. Για να ενεργοποιήσουμε το System Activity Reporter (sar) δίνουμε τις εντολές:

 # gedit /etc/default/sysstat

ENABLED="true"

```
  GNU nano 2.5.3          File: /etc/default/sysstat

#
# Default settings for /etc/init.d/sysstat, /etc/cron.d/sysstat
# and /etc/cron.daily/sysstat files
#

# Should sadc collect system activity informations? Valid values
# are "true" and "false". Please do not put other values, they
# will be overwritten by debconf!
ENABLED="true"

                          [ Wrote 10 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

 # /etc/init.d/sysstat start

Μετά τη διεξαγωγή της αρχικής αναγνώρισης των στοιχείων του συστήματος, θα πρέπει να εντοπίσουμε τους χρήστες που είναι συνδεδεμένοι στο σύστημα, τόσο τοπικά όσο και απομακρυσμένα. Έτσι εντοπίζουμε και τυχόν άλλα συστήματα που έχουν τυχόν παραβιαστεί, και παίρνουμε πληροφορίες που μπορούμε να συσχετίσουμε με άλλες που έχουμε συγκεντρώσει ή θα συλλέξουμε σε επόμενο βήμα. Αναζητούμε τις παρακάτω πληροφορίες που αφορούν συνδεδεμένους χρήστες όπως όνομα χρήστη (Username), από που συνδέονται (τοπικά ή απομακρυσμένα), διάρκεια της σύνδεσης, κοινόχρηστα αρχεία ή άλλους πόρους στους οποίους είχε πρόσβαση ο κακόβουλος χρήστης, διεργασίες σχετικές με τον χρήστη και την δικτυακή του δραστηριότητα. Οι εντολές που χρησιμοποιούμε αναζητούν τις πληροφορίες στο αρχείο "utmp". Πρόκειται για μία απλή βάση δεδομένων με πληροφορίες όπως λογαριασμός χρήστη (user account), διάρκεια και από που συνδέθηκε (τοπικά ή απομακρυσμένα) για κάθε σύνδεση (σύνοδο).

 # who

```
root@ubuntu:/home/user2# who
user2    tty7         2017-10-03 14:15 (:0)
```

 # w

```
root@ubuntu:/home/user2# w
 14:29:44 up 14 min,  1 user,  load average: 0.00, 0.12, 0.16
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
user2    tty7     :0               14:15   14:33  10.29s  0.16s /sbin/upstart -
```

 # users

```
root@ubuntu:/home/user2# users
user2
```

 # lastlog | grep -v Never

 # last
 # finger
 # pinky

```
user2@ubuntu:~$ finger
Login     Name          Tty      Idle  Login Time   Office     Office Phone
user2     ubuntu16.04   tty7       40  Oct  7 22:40 (:0)
user2@ubuntu:~$ pinky
Login    Name                 TTY      Idle   When             Where
user2    ubuntu16.04          tty7     00:41  2017-10-07 22:40 :0
user2@ubuntu:~$ last
user2    tty7         :0               Sat Oct  7 22:40    gone - no logout
reboot   system boot  4.10.0-28-generi Sat Oct  7 22:40   still running
user2    tty7         :0               Wed Oct  4 12:30 - crash (3+10:09)
reboot   system boot  4.10.0-28-generi Wed Oct  4 12:30   still running
user2    tty7         :0               Wed Oct  4 10:32 - down   (01:56)
reboot   system boot  4.10.0-28-generi Wed Oct  4 10:32 - 12:28  (01:56)
user2    tty7         :0               Tue Oct  3 17:56 - down   (00:01)
reboot   system boot  4.10.0-28-generi Tue Oct  3 17:56 - 17:58  (00:01)
user2    tty7         :0               Tue Oct  3 14:15 - down   (03:23)
reboot   system boot  4.10.0-28-generi Tue Oct  3 14:15 - 17:39  (03:24)
user2    tty7         :0               Tue Oct  3 06:20 - down   (00:46)
reboot   system boot  4.10.0-28-generi Tue Oct  3 06:20 - 07:06  (00:46)
user2    tty7         :0               Tue Oct  3 05:43 - crash  (00:36)
reboot   system boot  4.10.0-28-generi Tue Oct  3 05:39 - 07:06  (01:27)

wtmp begins Tue Oct  3 05:39:34 2017
```

Εντολές που σχετίζονται με τους χρήστες που έχουν πρόσβαση στο σύστημα. Χρήστες που έχουν λογαριασμό στον συγκεκριμένο υπολογιστή, εντολή:

sort -nk3 -t: /etc/passwd

```
root@ubuntu:/home/user2# sort -nk3 -t: /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
n
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/fal
se
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/
false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
```

Χρήστες που έχουν δικαιώματα root (ένας μόνο θα πρέπει να υπάρχει), εντολή:

egrep ':0+:' /etc/passwd

```
root@ubuntu:~# egrep ':0+:' /etc/passwd
root:x:0:0:root:/root:/bin/bash
user:x:0:0:nobody,,,,:/:/bin/bash
root@ubuntu:~#
```

 # getent passwd | egrep ':0+:'

```
root@ubuntu:~# getent passwd | egrep ':0+:'
root:x:0:0:root:/root:/bin/bash
user:x:0:0:nobody,,,,:/:/bin/bash
root@ubuntu:~#
```

Στην παραπάνω περίπτωση είναι ύποπτη η παρουσία δύο χρηστών με δικαιώματα root. Επίσης αναζητώ αρχεία που ανήκουν σε χρήστες που δεν έχουν δικαίωμα πρόσβασης πλέον στον υπολογιστή:
 # find / -nouser –print

```
root@ubuntu:/home/user2# find / -nouser -print
find: ‘/proc/2740/task/2740/fd/6’: No such file or directory
find: ‘/proc/2740/task/2740/fdinfo/6’: No such file or directory
find: ‘/proc/2740/fd/5’: No such file or directory
find: ‘/proc/2740/fdinfo/5’: No such file or directory
find: ‘/mnt/hgfs’: Protocol error
find: ‘/run/user/1000/gvfs’: Permission denied
root@ubuntu:/home/user2#
```

Για να δούμε σε ποιο group ανήκουν οι χρήστες δίνουμε τις παρακάτω εντολές:

 # getent passwd | cut -d : -f 1 | xargs groups
 # getent group root wheel adm admin
 # getent passwd <user>
 # getent group 1000
 # getent passwd 0

```
user2@ubuntu:~$ getent passwd 0
root:x:0:0:root:/root:/bin/bash
user2@ubuntu:~$ getent group 1000
user2:x:1000:
```

Ο εντοπισμός ύποπτων αρχείων γίνεται με τις εντολές

 # find / -nouser -print (εντοπίζει ορφανά αρχεία)
 # find / -size +10000k -print (εντοπίζει μεγάλα αρχεία)
 # find / -name ".. " -print
 # find / -name ". " -print
 # find / -name " " –print

Οι συνδέσεις δικτύου και η δικτυακή δραστηριότητα του συστήματος μπορούν να αποκαλύψουν σημαντικές πληροφορίες σχετικά με τη σύνδεση ενός κακόβουλου στο σύστημα, συμπεριλαμβανομένης της θέσης του απομακρυσμένου διακομιστή που συνδέθηκε, τη συλλογή δεδομένων που επιχείρησε ο κακόβουλος και αν το σύστημα χρησιμοποιείται ως κέντρο ελέγχου ενός botnet[11]. Κατά την εξέταση ενός δυνητικά μολυσμένου υπολογιστή, θα πρέπει να συλλέξουμε τις ακόλουθες πληροφορίες σχετικά με τη δραστηριότητα του δικτύου:

- Τις ενεργές συνδέσεις δικτύου
- Το Address Resolution Protocol (ARP) cache
- Το εσωτερικό δίκτυο δρομολόγησης (Internal routing table)

Το βασικό εργαλείο για να δούμε τις συνδέσεις ενός υπολογιστή είναι το netstat. Η βασική εντολή netstat –anp μας επιστρέφει τις παρακάτω πληροφορίες:

- εάν η σύνδεση είναι Transmission Control Protocol (TCP) ή User Datagram Protocol (UDP)
- Την κατάσταση της σύνδεσης
- Την εξωτερική IP
- Τον αριθμό της διεργασίας [process ID (PID)]

 # netstat –anp

```
root@ubuntu:~# netstat -anp|grep -i established
Active Internet connections (servers and established)
tcp        0      0 192.168.1.7:46939       172.217.16.206:80       ESTABLISHED 5230/firefox
tcp        0      0 192.168.1.7:34811       216.58.208.46:443       ESTABLISHED 5230/firefox
tcp        0      0 192.168.1.7:46096       91.189.90.41:80         ESTABLISHED 5230/firefox
tcp        0      0 192.168.1.7:49700       172.217.18.14:443       ESTABLISHED 5230/firefox
Active UNIX domain sockets (servers and established)
```

 # netstat –pantu

[11] Ως botnet ορίζεται ένα δίκτυο υπολογιστών, το οποίο ελέγχεται εξ αποστάσεως από τον λεγόμενο botmaster χωρίς τη γνώση ή την έγκριση των κατόχων των μεμονωμένων υπολογιστών. Οι υπολογιστές που είναι μέλη του δικτύου αυτού ονομάζονται ζόμπι.

```
root@ubuntu:~# netstat -pantu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      2007/cupsd
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN      1214/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1204/sshd
tcp        1      0 172.17.22.23:45509      162.213.33.48:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:44980      162.213.33.50:443       CLOSE_WAIT  3002/gvfsd-http
tcp        0      0 172.17.22.23:54448      216.58.198.142:443      ESTABLISHED 9267/firefox
tcp        1      0 172.17.22.23:45512      162.213.33.48:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:45515      162.213.33.48:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:44983      162.213.33.50:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:44986      162.213.33.50:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:49153      162.213.33.49:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:45861      162.213.33.48:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:49507      162.213.33.49:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:45506      162.213.33.48:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:49165      162.213.33.49:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:49159      162.213.33.49:443       CLOSE_WAIT  3002/gvfsd-http
tcp        0      0 172.17.22.23:49452      216.58.210.14:443       ESTABLISHED 9267/firefox
tcp        1      0 172.17.22.23:49156      162.213.33.49:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:49515      162.213.33.49:443       CLOSE_WAIT  2833/unity-scope-ho
tcp        1      0 172.17.22.23:49162      162.213.33.49:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:45858      162.213.33.48:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:44977      162.213.33.50:443       CLOSE_WAIT  3002/gvfsd-http
tcp        1      0 172.17.22.23:45330      162.213.33.50:443       CLOSE_WAIT  3002/gvfsd-http
tcp6       0      0 ::1:631                 :::*                    LISTEN      2007/cupsd
tcp6       0      0 :::22                   :::*                    LISTEN      1204/sshd
tcp6       1      0 ::1:51436               ::1:631                 CLOSE_WAIT  1333/cups-browsed
udp        0      0 127.0.1.1:53            0.0.0.0:*                           1214/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*                           28331/dhclient
udp        0      0 0.0.0.0:631             0.0.0.0:*                           1333/cups-browsed
udp        0      0 0.0.0.0:61123           0.0.0.0:*                           28331/dhclient
udp        0      0 0.0.0.0:60629           0.0.0.0:*                           768/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           768/avahi-daemon: r
udp6       0      0 :::1648                 :::*                                28331/dhclient
udp6       0      0 :::5353                 :::*                                768/avahi-daemon: r
udp6       0      0 :::51951                :::*                                768/avahi-daemon: r
```

Οι συνδέσεις του δικτύου μπορούν να αποκαλυφθούν και με την εντολή ss (socket statistics).
$ ss | less (Όλες οι συνδέσεις)
$ ss -t (Μόνο tcp)
$ ss -ua (Μόνο udp)
$ ss -lnt (listen ports)
$ ss -ltp (pid)
$ ss -s (statistics)

```
user2@ubuntu:~$ ss -t
State       Recv-Q Send-Q Local Address:Port                 Peer Address:Port

user2@ubuntu:~$ ss -ua
State       Recv-Q Send-Q Local Address:Port                 Peer Address:Port

UNCONN      0      0          *:51657                    *:*
UNCONN      0      0      *%ens33:58911                    *:*

UNCONN      0      0      127.0.1.1:domain                 *:*

UNCONN      0      0          *:bootpc                   *:*
UNCONN      0      0          *:ipp                      *:*
UNCONN      0      0          *:mdns                     *:*
UNCONN      0      0         :::39119                   :::*
UNCONN      0      0         :::mdns                    :::*
user2@ubuntu:~$ ss -s
Total: 1372 (kernel 0)
TCP:   1 (estab 0, closed 0, orphaned 0, synrecv 0, timewait 0/0), ports 0

Transport Total     IP        IPv6
*         0         -         -
RAW       1         0         1
UDP       8         6         2
TCP       1         1         0
INET      10        7         3
FRAG      0         0         0
```

Κάποιοι τύποι ιομορφικού λογισμικού έχουν την δυνατότητα να αλλάζουν τον πίνακα δρομολόγησης στο σύστημα, ώστε να αλλάξει την δρομολόγηση των πακέτων. Επιπλέον, οι κακόβουλοι χρήστες μπορεί να δημιουργήσουν συνδέσεις εικονικού ιδιωτικού δικτύου (Virtual Private Network-VPN) με έναν απομακρυσμένο διακομιστή για να μεταφέρουν κλεμμένα δεδομένα μέσω μιας κρυπτογραφημένης συνόδου, που δεν μπορεί να παρατηρηθεί-εντοπιστεί καθαρά από τα συστήματα επιτήρησης του δικτύου.

$ netstat -nr
$ route –e

```
root@ubuntu:~# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         172.17.22.1     0.0.0.0         UG        0 0          0 eth0
172.17.22.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@ubuntu:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.17.22.1     0.0.0.0         UG    0      0        0 eth0
172.17.22.0     0.0.0.0         255.255.255.0   U     1      0        0 eth0
```

Η ARP cache διατηρεί πληροφορίες σχετικά με τις τρέχουσες και πρόσφατες συνδέσεις ανάμεσα στους υπολογιστές του τοπικού δικτύου. Η εντολή arp εμφανίζει την ARP cache σε ένα Linux σύστημα και παρουσιάζει την λίστα των Ips σχετιζόμενες με τις διευθύνσεις MAC του τοπικού δικτύου και με τις οποίες πρόσφατα συνδέθηκε ο συγκεκριμένος υπολογιστής.

$ arp -a

```
root@ubuntu:/home/user2# arp -a
? (192.168.110.254) at 00:50:56:eb:43:b8 [ether] on ens33
? (192.168.110.2) at 00:50:56:ec:80:28 [ether] on ens33
```

$ arp -n

```
root@ubuntu:/home/user2# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.110.254          ether   00:50:56:eb:43:b8   C                     ens33
192.168.110.2            ether   00:50:56:ec:80:28   C                     ens33
```

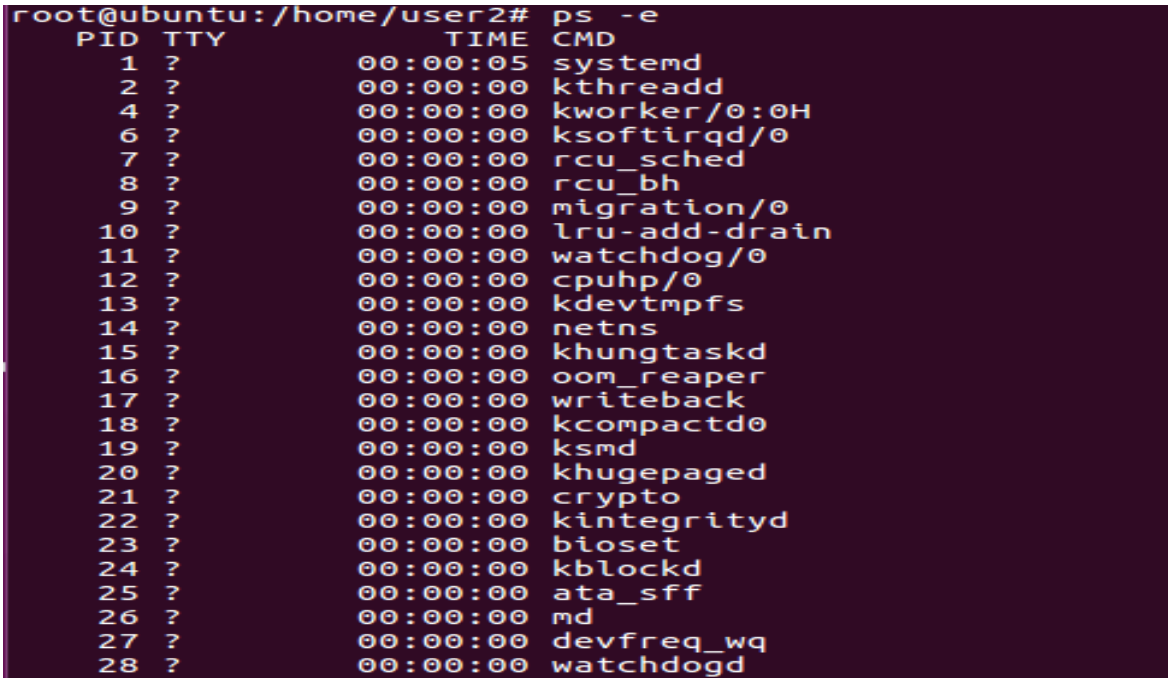
$ cat /proc/net/arp

```
root@ubuntu:/home/user2# cat /proc/net/arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.110.254  0x1         0x2         00:50:56:eb:43:b8     *        ens33
192.168.110.2    0x1         0x2         00:50:56:ec:80:28     *        ens33
```

<u>Τρέχουσες Διεργασίες</u>

Η συλλογή πληροφοριών που αφορούν τις διεργασίες, είναι πολύ σημαντική ενέργεια στην διαδικασία της διαχείρισης ενός κυβερνοπεριστατικού. Μόλις το ιομορφικό λογισμικό εκτελεστεί σε έναν υπολογιστή το πιο πιθανό είναι να εμφανιστεί ως μία διεργασία. Οι πληροφορίες που αναζητάμε είναι: Όνομα διεργασίας και PID, χρονικό πλαίσιο, χρήση μνήμης, αντιστοιχία διεργασίας με εκτελέσιμο αρχείο, αντιστοιχία διεργασίας με χρήστη, διεργασίες παιδιά (Child processes), καλούμενες βιβλιοθήκες και εξαρτώμενες εφαρμογές, παραμέτρους των εντολών (Command-line arguments), το περιεχόμενο της μνήμης της διεργασίας και η σχέση της διεργασίας με την κατάσταση του συστήματος και τα αποδεικτικά στοιχεία. Για να έχουμε μία λίστα των διεργασιών που εκτελούνται χρησιμοποιούμε την εντολή – εργαλείο ps.

$ ps - e



Για να έχουμε τον χρόνο και γενικότερα την ιστορία των διεργασιών, δίνουμε την εντολή:

$ ps -ef

$ ps aux

Οι εντολές αυτές μας δείχνουν ανάμεσα στις άλλες πληροφορίες τα ονόματα και τις σχετιζόμενες PIDs. Με την παρακάτω εντολή παίρνουμε πληροφορίες σχετικά με τις τρέχουσες διεργασίες, PIDs, και την χρήση μνήμης και CPU.

$ ps axu

```
user2@ubuntu:~$ ps axu
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.2  0.3 185216  3972 ?        Ss   13:38   0:02 /sbin/init aut
root          2  0.0  0.0      0     0 ?        S    13:38   0:00 [kthreadd]
root          4  0.0  0.0      0     0 ?        S<   13:38   0:00 [kworker/0:0H]
root          6  0.1  0.0      0     0 ?        S    13:38   0:00 [ksoftirqd/0]
root          7  0.0  0.0      0     0 ?        S    13:38   0:00 [rcu_sched]
root          8  0.0  0.0      0     0 ?        S    13:38   0:00 [rcu_bh]
root          9  0.0  0.0      0     0 ?        S    13:38   0:00 [migration/0]
root         10  0.0  0.0      0     0 ?        S<   13:38   0:00 [lru-add-drain
root         11  0.0  0.0      0     0 ?        S    13:38   0:00 [watchdog/0]
root         12  0.0  0.0      0     0 ?        S    13:38   0:00 [cpuhp/0]
root         13  0.0  0.0      0     0 ?        S    13:38   0:00 [kdevtmpfs]
root         14  0.0  0.0      0     0 ?        S<   13:38   0:00 [netns]
root         15  0.0  0.0      0     0 ?        S    13:38   0:00 [khungtaskd]
root         16  0.0  0.0      0     0 ?        S    13:38   0:00 [oom_reaper]
root         17  0.0  0.0      0     0 ?        S<   13:38   0:00 [writeback]
root         18  0.0  0.0      0     0 ?        S    13:38   0:00 [kcompactd0]
root         19  0.0  0.0      0     0 ?        SN   13:38   0:00 [ksmd]
root         20  0.0  0.0      0     0 ?        SN   13:38   0:00 [khugepaged]
root         21  0.0  0.0      0     0 ?        S<   13:38   0:00 [crypto]
root         22  0.0  0.0      0     0 ?        S<   13:38   0:00 [kintegrityd]
root         23  0.0  0.0      0     0 ?        S<   13:38   0:00 [bioset]
root         24  0.0  0.0      0     0 ?        S<   13:38   0:00 [kblockd]
root         25  0.0  0.0      0     0 ?        S<   13:38   0:00 [ata_sff]
root         26  0.0  0.0      0     0 ?        S<   13:38   0:00 [md]
root         27  0.0  0.0      0     0 ?        S<   13:38   0:00 [devfreq_wq]
root         28  0.0  0.0      0     0 ?        S<   13:38   0:00 [watchdogd]
root         30  0.0  0.0      0     0 ?        S    13:38   0:00 [kworker/0:1]
root         32  0.0  0.0      0     0 ?        S    13:38   0:00 [kauditd]
```

Η εφαρμογή pidstat μπορεί να μας δώσει πολλές πληροφορίες σχετικά με την δράση – χρήση μιας διεργασίας.

$ pidstat -p <target pid>
Παράμετρος -r -report page faults
Παράμετρος: -s -stack utilization
Παράμετρος: -d -I/O statistics

```
root@ubuntu:~# pidstat -p 28020
Linux 3.13.0-32-generic (ubuntu)        06/11/2016      _x86_64_        (1 CPU)

08:57:29 AM   UID       PID    %usr %system  %guest    %CPU   CPU  Command
08:57:29 AM     0     28020    0.00    0.00    0.00    0.00     0  sh
```

Αντιστοίχιση διεργασιών και εκτελέσιμων

Για να εντοπίσουμε με ποιο εκτελέσιμο σχετίζεται μία διεργασία χρησιμοποιούμε τις παρακάτω εντολές:

$ whereis –b <exec>
$ which -a <exec>

Η εντολή whereis εντοπίζει πηγαίο κώδικα ή το εκτελέσιμο του ιομορφικού κώδικα/εκτελέσιμο. Παρόμοια και η εντολή which μας δείχνει την πλήρη διαδρομή (full system path) του εκτελέσιμου αρχείου. Ο διακόπτης -a μας δείχνει όλα τα

εκτελέσιμα που ταιριάζουν στην ερώτησή μας και βρίσκονται στο μονοπάτι (PATH) όχι απλά το πρώτο που θα εντοπιστεί.

```
root@ubuntu:/home/user2# which -a bash
/bin/bash
root@ubuntu:/home/user2# which -a script
/usr/bin/script
```

Ακολούθως θέλουμε να συσχετίσουμε διεργασίες με τους αντίστοιχους users με σκοπό να εντοπίσουμε ποιοι τρέχουν διεργασίες με αναβαθμισμένα δικαιώματα, κάτι που αποτελεί ένδειξη παραβίασης. Αυτό επιτυγχάνεται με την εξής εντολή:

$ ps -U <username> -u <username>

Μια πιο ειδική αναζήτηση πληροφοριών είναι η εντολή:

$ ps -eo pid,user,group,args,etime,lstart |grep '<ύποπτη pid>'

Όταν εντοπίζουμε μία ιομορφική διεργασία, επόμενο βήμα είναι να διακρίνουμε την ιεραρχική της σχέση, να βρούμε τον γονέα και τα παιδιά της. Οι εντολές που ακολουθούν μας βοηθούν σε αυτό.

$ ps -ejH

```
root@ubuntu:/home/user2# ps -ejH
    PID    PGID     SID TTY          TIME CMD
      2       0       0 ?        00:00:00 kthreadd
      4       0       0 ?        00:00:00   kworker/0:0H
      6       0       0 ?        00:00:00   ksoftirqd/0
      7       0       0 ?        00:00:01   rcu_sched
      8       0       0 ?        00:00:00   rcu_bh
      9       0       0 ?        00:00:00   migration/0
     10       0       0 ?        00:00:00   lru-add-drain
     11       0       0 ?        00:00:00   watchdog/0
     12       0       0 ?        00:00:00   cpuhp/0
     13       0       0 ?        00:00:00   kdevtmpfs
     14       0       0 ?        00:00:00   netns
     15       0       0 ?        00:00:00   khungtaskd
     16       0       0 ?        00:00:00   oom_reaper
     17       0       0 ?        00:00:00   writeback
     18       0       0 ?        00:00:00   kcompactd0
     19       0       0 ?        00:00:00   ksmd
     20       0       0 ?        00:00:00   khugepaged
     21       0       0 ?        00:00:00   crypto
     22       0       0 ?        00:00:00   kintegrityd
     23       0       0 ?        00:00:00   bioset
     24       0       0 ?        00:00:00   kblockd
     25       0       0 ?        00:00:00   ata_sff
     26       0       0 ?        00:00:00   md
     27       0       0 ?        00:00:00   devfreq_wq
     28       0       0 ?        00:00:00   watchdogd
     32       0       0 ?        00:00:00   kauditd
     33       0       0 ?        00:00:01   kswapd0
     34       0       0 ?        00:00:00   vmstat
     35       0       0 ?        00:00:00   bioset
     36       0       0 ?        00:00:00   ecryptfs-kthrea
```

$ ps axjf

```
root@ubuntu:/home/user2# ps axjf
  PPID    PID   PGID    SID TTY        TPGID STAT   UID   TIME COMMAND
     0      2      0      0 ?           -1 S        0   0:00 [kthreadd]
     2      4      0      0 ?           -1 S<       0   0:00  \_ [kworker/0:0H]
     2      6      0      0 ?           -1 S        0   0:00  \_ [ksoftirqd/0]
     2      7      0      0 ?           -1 S        0   0:01  \_ [rcu_sched]
     2      8      0      0 ?           -1 S        0   0:00  \_ [rcu_bh]
     2      9      0      0 ?           -1 S        0   0:00  \_ [migration/0]
     2     10      0      0 ?           -1 S<       0   0:00  \_ [lru-add-drain
     2     11      0      0 ?           -1 S        0   0:00  \_ [watchdog/0]
     2     12      0      0 ?           -1 S        0   0:00  \_ [cpuhp/0]
     2     13      0      0 ?           -1 S        0   0:00  \_ [kdevtmpfs]
     2     14      0      0 ?           -1 S<       0   0:00  \_ [netns]
     2     15      0      0 ?           -1 S        0   0:00  \_ [khungtaskd]
     2     16      0      0 ?           -1 S        0   0:00  \_ [oom_reaper]
     2     17      0      0 ?           -1 S<       0   0:00  \_ [writeback]
     2     18      0      0 ?           -1 S        0   0:00  \_ [kcompactd0]
     2     19      0      0 ?           -1 SN       0   0:00  \_ [ksmd]
     2     20      0      0 ?           -1 SN       0   0:00  \_ [khugepaged]
     2     21      0      0 ?           -1 S<       0   0:00  \_ [crypto]
     2     22      0      0 ?           -1 S<       0   0:00  \_ [kintegrityd]
     2     23      0      0 ?           -1 S<       0   0:00  \_ [bioset]
     2     24      0      0 ?           -1 S<       0   0:00  \_ [kblockd]
     2     25      0      0 ?           -1 S<       0   0:00  \_ [ata_sff]
     2     26      0      0 ?           -1 S<       0   0:00  \_ [md]
     2     27      0      0 ?           -1 S<       0   0:00  \_ [devfreq_wq]
     2     28      0      0 ?           -1 S<       0   0:00  \_ [watchdogd]
     2     32      0      0 ?           -1 S        0   0:00  \_ [kauditd]
     2     33      0      0 ?           -1 S        0   0:01  \_ [kswapd0]
     2     34      0      0 ?           -1 S<       0   0:00  \_ [vmstat]
     2     35      0      0 ?           -1 S<       0   0:00  \_ [bioset]
     2     36      0      0 ?           -1 S        0   0:00  \_ [ecryptfs-kthr
```

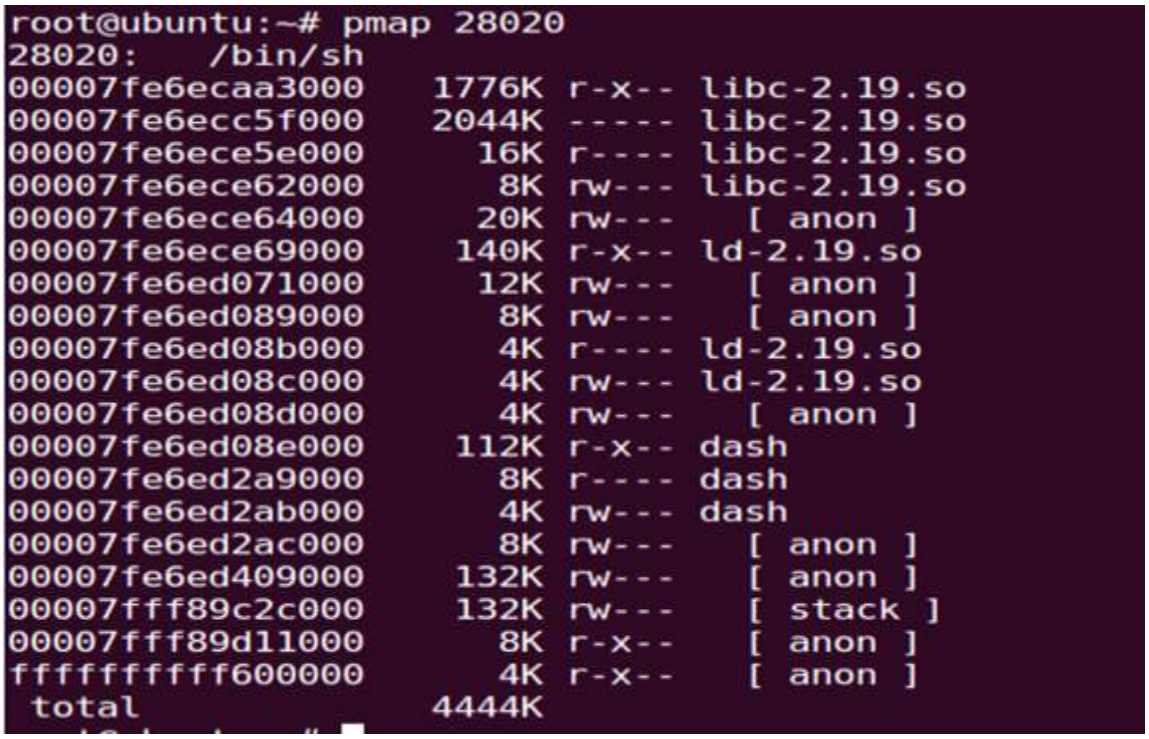
$ pstree -a
$ pstree –al
$ pstree –ah

```
user2@ubuntu:~$ pstree -a
systemd auto noprompt
  ├─ModemManager
  │    ├─{gdbus}
  │    └─{gmain}
  ├─NetworkManager --no-daemon
  │    ├─dhclient -d -q -sf /usr/lib/NetworkManager/nm-dhcp-helper -pf...
  │    ├─dnsmasq --no-resolv --keep-in-foreground --no-hosts ...
  │    ├─{gdbus}
  │    └─{gmain}
  ├─accounts-daemon
  │    ├─{gdbus}
  │    └─{gmain}
  ├─acpid
  ├─agetty --noclear tty1 linux
  ├─avahi-daemon
  │    └─avahi-daemon
  ├─colord
  │    ├─{gdbus}
  │    └─{gmain}
  ├─cron -f
  ├─cups-browsed
  │    ├─{gdbus}
  │    └─{gmain}
  ├─dbus-daemon --system --address=systemd: --nofork --nopidfile--systemd-
  ├─fwupd
  │    ├─3*[{GUsbEventThread}]
  │    ├─{fwupd}
  │    ├─{gdbus}
```

Μία εφαρμογή που μας επιτρέπει να δούμε τις βιβλιοθήκες που χρησιμοποιεί ένα

εκτελέσιμο είναι το pmap.

$ pmap PID



Ο κατάλογος /proc

Ένα linux λειτουργικό σύστημα έχει τον “/proc” κατάλογο (directory) στον οποίο περιέχει ένα εικονικό αρχείο συστήματος το οποίο παρουσιάζει την τρέχουσα κατάσταση του πυρήνα. Οι πληροφορίες είναι σημαντικές από την κατάσταση των διεργασιών μέχρι και παραμέτρους της γραμμής εντολών. Ο κατάλογος /proc έχει ιεραρχική δομή και σημαντικές πληροφορίες αναζητούμε στους παρακάτω υποκαταλόγους:

Στον “/proc/<PID>/cmdline” περιέχει τις παραμέτρους των γραμμών εντολών.

Στον “/proc/<PID>/cwd” βρίσκεται το τρέχον directory μιας διεργασίας.

Στον “/proc/<PID>/environ” βρίσκονται οι μεταβλητές περιβάλλοντος της διεργασίας.

Στον “/proc/<PID>/exe” πρόκειται για symbolic link στο εκτελέσιμο αρχείο που σχετίζεται με την διεργασία.

```
user2@ubuntu:~$ ps
   PID TTY          TIME CMD
  2320 pts/0    00:00:00 bash
 27587 pts/0    00:00:00 ps
user2@ubuntu:~$ cd /proc/2320/
user2@ubuntu:/proc/2320$ ls
attr             cwd       map_files   oom_adj        sessionid  timers
autogroup        environ   maps        oom_score      setgroups  timerslack_ns
auxv             exe       mem         oom_score_adj  smaps      uid_map
cgroup           fd        mountinfo   pagemap        stack      wchan
clear_refs       fdinfo    mounts      personality    stat
cmdline          gid_map   mountstats  projid_map     statm
comm             io        net         root           status
coredump_filter  limits    ns          sched          syscall
cpuset           loginuid  numa_maps   schedstat      task
user2@ubuntu:/proc/2320$ cat cmdline
bashuser2@ubuntu:/proc/2320$ cd cwd
user2@ubuntu:/proc/2320/cwd$ ls
attr             cwd       map_files   oom_adj        sessionid  timers
autogroup        environ   maps        oom_score      setgroups  timerslack_ns
auxv             exe       mem         oom_score_adj  smaps      uid_map
cgroup           fd        mountinfo   pagemap        stack      wchan
clear_refs       fdinfo    mounts      personality    stat
cmdline          gid_map   mountstats  projid_map     statm
comm             io        net         root           status
coredump_filter  limits    ns          sched          syscall
cpuset           loginuid  numa_maps   schedstat      task
```

Συσχέτιση Θυρών με Διεργασίες και προγράμματα

Όταν εξετάζουμε τις ανοικτές πόρτες (open ports) θα πρέπει να αναζητήσουμε τις παρακάτω πληροφορίες:

- Τοπική διεύθυνση IP και την πόρτα
- Απομακρυσμένη διεύθυνση IP και την πόρτα
- Όνομα απομακρυσμένου υπολογιστή
- Πρωτόκολλο σύνδεσης
- Κατάσταση της σύνδεσης
- Όνομα της διεργασίας και PID
- Εκτελέσιμο πρόγραμμα που συνδέεται με τη διεργασία
- Διαδρομή εκτελέσιμου προγράμματος
- Το όνομα χρήστη που σχετίζονται με τη διεργασία / πρόγραμμα

$ netstat -pantu

```
root@ubuntu:/proc/2465# netstat -pantu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
1158/dnsmasq
udp        0      0 0.0.0.0:45895           0.0.0.0:*
1158/dnsmasq
udp        0      0 127.0.1.1:53            0.0.0.0:*
1158/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*
2903/dhclient
udp        0      0 0.0.0.0:631             0.0.0.0:*
936/cups-browsed
udp        0      0 0.0.0.0:55470           0.0.0.0:*
860/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*
860/avahi-daemon: r
udp        0      0 127.0.0.1:33056         127.0.1.1:53            ESTABLISHED
465/systemd-timesyn
udp6       0      0 :::60008                :::*
860/avahi-daemon: r
udp6       0      0 :::5353                 :::*
860/avahi-daemon: r
```

Εντοπισμός ανοικτών αρχείων και πρόσβαση

Διακρίνοντας ποια διεργασία έχει πρόσβαση σε συγκεκριμένο αρχείο, μπορούμε να εντοπίσουμε σε ποιο αρχείο “γράφει” ένας keylogger ή γενικά μία backdoor. Η lsof εντολή αποκαλύπτει αρχεία και sockets που έχει πρόσβαση ένα πρόγραμμα που εκτελείται.

$ lsof -i -n -P
$ lsof -P -n -i -V
$ lsof -n -P -V
$ lsof +L1
$ lsof -i

```
root@ubuntu:/proc/2465# lsof -i -n -P
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-t  465 systemd-timesync   13u  IPv4 138794      0t0  UDP 127.0.0.1:39413
->127.0.1.1:53
avahi-dae  860           avahi   12u  IPv4  18620      0t0  UDP *:5353
avahi-dae  860           avahi   13u  IPv6  18621      0t0  UDP *:5353
avahi-dae  860           avahi   14u  IPv4  18622      0t0  UDP *:55470
avahi-dae  860           avahi   15u  IPv6  18623      0t0  UDP *:60008
cups-brow  936            root    8u  IPv4  19573      0t0  UDP *:631
dnsmasq   1158          nobody    4u  IPv4  20863      0t0  UDP 127.0.1.1:53
dnsmasq   1158          nobody    5u  IPv4  20864      0t0  TCP 127.0.1.1:53 (L
ISTEN)
dnsmasq   1158          nobody   11u  IPv4 124906      0t0  UDP *:45895
dhclient  2903            root    6u  IPv4 124891      0t0  UDP *:68
```

Εντοπισμός Ύποπτων Υπηρεσιών

Όταν συγκεντρώνουμε πληροφορίες για τις εκτελούμενες υπηρεσίες, αναζητούμε τα παρακάτω:

- Όνομα υπηρεσίας

- Το εμφανιζόμενο όνομα της υπηρεσίας
- Κατάσταση
- Διαμόρφωση εκκίνησης
- Περιγραφή υπηρεσίας
- Εξαρτήσεις
- Εκτελέσιμο πρόγραμμα που συνδέεται με την υπηρεσία
- Αναγνωριστικό διαδικασίας PID
- Διαδρομή εκτελέσιμου προγράμματος
- Όνομα Χρήστη που συνδέεται με την υπηρεσία

$ service --status-all |grep +
Εντολή για να δούμε ποιες υπηρεσίες ξεκινάνε στην επανεκκίνηση:
$ grep -i 'runlevel' /etc/init/* | awk '!/#/ && /start on/ && /2/ {gsub("/"," "); print $0 }' | cut -d ' ' -f4-

$grep -i 'runlevel' /etc/init/* | awk '/start on/ && /2/ {gsub("/"," "); gsub(":", " ");gsub(".conf"," "); print $3 }'

Εξέταση Ενοτήτων Πυρήνα (Kernel Modules)

Ένα ιομορφικό λογισμικό μπορεί να “φορτωθεί” ως kernel module. Με την παρακάτω εντολή βλέπουμε ποια modules έκτελούνται:
lsmod | head

```
root@ubuntu:~# lsmod | head
Module                  Size  Used by
binfmt_misc            20480  1
vmw_vsock_vmci_transport    28672  1
vsock                  36864  2 vmw_vsock_vmci_transport
vmw_balloon            20480  0
coretemp               16384  0
crct10dif_pclmul       16384  0
crc32_pclmul           16384  0
ghash_clmulni_intel    16384  0
pcbc                   16384  0
root@ubuntu:~#
```

Ανάκτηση Ιστορικού Εντολών

Στο λειτουργικό Ubuntu το κέλυφος (shell) παράγει και διατηρεί ένα ιστορικό εντολών για κάθε λογαριασμό χρήστη. Μπορούμε μέσα από αυτό να αποκαλύψουμε την δράση ενός κακόβουλου χρήστη. Στο Ubuntu μπορώ να ελέγξω τα περιεχόμενα του αντίστοιχου αρχείου με την εντολή:

$ cat .bash_history

```
user2@ubuntu:~$ cat .bash_history
sudo apt-get install dwarfdump
sudo apt-get install volatility
volatility
volatility -h
uname -a
script
date
hostname -f
sudo su
ifconfig
sudo apt-get install lime-forensics-dkms
lime
mount
cd /media
ls
cd user2
ls
ifconfig
```

Επιθεώρηση Κοινοχρήστων Δικτύου (Network Shares)

Με σκοπό την απλοποίηση της διαχείρισης πολλές φορές αποθηκεύουμε πολλά δεδομένα απομακρυσμένα σε κεντρικούς εξυπηρετητές (servers). Σε αυτές τις δικτυακές περιοχές μπορεί κάποιος να αποθηκεύσει ιομορφικά αρχεία, που μπορούν να μας αποκαλύψουν σημαντικές πληροφορίες. Με τις παρακάτω εντολές ελέγχουμε αυτές τις περιοχές:

$ cat /proc/mounts

```
user2@ubuntu:~$ cat /proc/mounts
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,nosuid,relatime,size=475172k,nr_inodes=118793,mode=755 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,noexec,relatime,size=99488k,mode=755 0 0
/dev/sda1 / ext4 rw,relatime,errors=remount-ro,data=ordered 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k 0 0
tmpfs /sys/fs/cgroup tmpfs ro,nosuid,nodev,noexec,mode=755 0 0
cgroup /sys/fs/cgroup/systemd cgroup rw,nosuid,nodev,noexec,relatime,xattr,relea
se_agent=/lib/systemd/systemd-cgroups-agent,name=systemd 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
cgroup /sys/fs/cgroup/net_cls,net_prio cgroup rw,nosuid,nodev,noexec,relatime,ne
t_cls,net_prio 0 0
cgroup /sys/fs/cgroup/cpuset cgroup rw,nosuid,nodev,noexec,relatime,cpuset 0 0
cgroup /sys/fs/cgroup/cpu,cpuacct cgroup rw,nosuid,nodev,noexec,relatime,cpu,cpu
acct 0 0
cgroup /sys/fs/cgroup/freezer cgroup rw,nosuid,nodev,noexec,relatime,freezer 0 0
cgroup /sys/fs/cgroup/memory cgroup rw,nosuid,nodev,noexec,relatime,memory 0 0
cgroup /sys/fs/cgroup/hugetlb cgroup rw,nosuid,nodev,noexec,relatime,hugetlb 0 0
cgroup /sys/fs/cgroup/devices cgroup rw,nosuid,nodev,noexec,relatime,devices 0 0
cgroup /sys/fs/cgroup/perf_event cgroup rw,nosuid,nodev,noexec,relatime,perf_eve
nt 0 0
cgroup /sys/fs/cgroup/pids cgroup rw,nosuid,nodev,noexec,relatime,pids 0 0
cgroup /sys/fs/cgroup/blkio cgroup rw,nosuid,nodev,noexec,relatime,blkio 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=32,pgrp=1,timeout=0,min
proto=5,maxproto=5,direct,pipe_ino=13711 0 0
mqueue /dev/mqueue mqueue rw,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,relatime 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,relatime 0 0
```

$ cat /proc/partitions

```
user2@ubuntu:~$ cat /proc/partitions
major minor  #blocks  name

   8        0   20971520 sda
   8        1   19921920 sda1
   8        2          1 sda2
   8        5    1046528 sda5
  11        0    1048575 sr0
user2@ubuntu:~$
```

$ cat /proc/swaps

```
user2@ubuntu:~$ cat /proc/swaps
Filename                                Type            Size    Used    Priority
/dev/sda5                               partition       1046524 426640  -1
user2@ubuntu:~$
```

Το εργαλειο df εμφανίζει το μέγεθος του διαθέσιμου χώρου στο δίσκο στο σύστημα αρχείων. Εάν δεν υπάρχει όνομα αρχείου, τότε εμφανίζεται ο διαθέσιμος χώρος σε όλα τα συστήματα αρχείων που έχουν φορτωθεί.

$ df -h
$ df –k

```
user2@ubuntu:/var/log/sysstat$ df -h
df: /mnt/hgfs: Protocol error
Filesystem      Size  Used Avail Use% Mounted on
udev            465M     0  465M   0% /dev
tmpfs            98M  8.7M   89M   9% /run
/dev/sda1        19G  6.0G   12G  34% /
tmpfs           486M  284K  486M   1% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           486M     0  486M   0% /sys/fs/cgroup
tmpfs            98M   76K   98M   1% /run/user/1000
```

Το εργαλείο du εκτελεί μία εκτίμηση της χρήσης χώρου από τα αρχεία

$ du -h /

```
4.0K    /root/.nano
4.0K    /root/.cache
4.0K    /root/.gnupg/private-keys-v1.d
32K     /root/.gnupg
56K     /root
16K     /lost+found
4.0K    /tmp/.Test-unix
28K     /tmp/vmware-root
4.0K    /tmp/.XIM-unix
4.0K    /tmp/gnome-software-5O4H7Y
4.0K    /tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-colord.service-1i8
a2M/tmp
8.0K    /tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-colord.service-1i8
a2M
4.0K    /tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-rtkit-daemon.servi
ce-KNChRz/tmp
8.0K    /tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-rtkit-daemon.servi
ce-KNChRz
4.0K    /tmp/.X11-unix
4.0K    /tmp/gnome-software-46SF7Y
4.0K    /tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-systemd-timesyncd.
service-E9Gzcx/tmp
8.0K    /tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-systemd-timesyncd.
service-E9Gzcx
4.0K    /tmp/.font-unix
4.0K    /tmp/gnome-software-KUIE7Y
4.0K    /tmp/gnome-software-12DZ7Y
4.0K    /tmp/gnome-software-Q7JE7Y
4.0K    /tmp/gnome-software-OFTU7Y
```

Εάν υπάρχει NFS (Network File System), θα πρέπει να εντοπίσουμε τα κοινόχρηστα αρχεία με τις παρακάτω εντολές:
$ cat /etc/samba/smb.conf
$ cat /etc/exports

Εξέταση Προγραμματισμένων Εργασιών

Ένα ιομορφικό λογισμικό μπορεί να ενεργοποιείται ανά τακτικά χρονικά διαστήματα. Οι προγραμματισμένες εργασίες μπορούν να παραμετροποιηθούν με την εντολή at ή με τα cronjobs. Συνεπώς θα πρέπει να ελέγχουμε τι υπάρχει στον scheduler και στο crontab ελέγχοντας τα σχετικά αρχεία:

/var/spool/cron/atjobs
/var/spool/cron/atspool
/etc/crontab
/etc/cron.daily
/etc/cron.hourly
/etc/cron.weekly
/etc/cron.monthly
/var/spool/cron/crontabs

Με τις αντίστοιχες εντολές:
crontab -u root -l
crontab -u <user> -l
cat /etc/crontab
ls /etc/cron.*

Εξέταση Περιεχομένων Πρόχειρου (Clipboard)

Το clipboard μπορεί να περιέχει σημαντικές πληροφορίες Με την χρήση ενός εργαλείου όπως το xclip μπορούμε να αποκαλύψουμε πληροφορίες, όπως:

- Ονόματα από domains
- Διευθύνσεις IP
- Διευθύνσεις ηλεκτρονικού ταχυδρομείου
- Ονόματα χρηστών και συνθηματικά
- Ονόματα από hosts
- Συζητήσεις Instant messenger ή περιεχόμενα ηλεκτρονικού ταχυδρομείου
- Εντολές

Εντοπισμός των αρχείων setuid και setgid

Ο κακόβουλος χρήστης όταν αποκτήσει πρόσβαση, τοποθετεί στο παραβιασμένο σύστημα αρχεία ή προγράμματα που του δίνουν την δυνατότητα σας απλός χρήστης να έχει δικαιώματα root. Τέτοια είναι τα αρχεία setuid και setgid. Θα πρέπει να αναγνωρίζουμε ποια από αυτά είναι τα νόμιμα αρχεία. Κάνουμε αναζήτηση αυτών των αρχείων:

$ find / -user root -perm -4000 -exec ls -ldb {} \;
$ find / \(-perm -u+s -o -perm -g+s \) -type f
$ find / -perm +6000 -type f -exec ls -ld {} \;

Εντοπισμός των suid αρχείων με τις εντολές:
$ find / -uid 0 -perm -4000 -print
$ find / -type f \(-perm -04000 -o -perm -02000 \)

```
user2@ubuntu:~$ sudo find / -uid 0 -perm -4000 -print
[sudo] password for user2:
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
/usr/sbin/pppd
/usr/lib/xorg/Xorg.wrap
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
find: ‘/proc/7947/task/7947/fd/6’: No such file or directory
find: ‘/proc/7947/task/7947/fdinfo/6’: No such file or directory
find: ‘/proc/7947/fd/5’: No such file or directory
```

Εντοπισμός των αρχείων που τροποποιήθηκαν τα τελευταία λεπτά με τις εντολές:
find / -mmin 5 (αρχεία που μεταβλήθηκαν τα τελευταία 5 λεπτά)

```
user2@ubuntu:~$ sudo find / -mmin 1
/tmp
/tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-systemd-hostnamed.service
C9MX9n
/tmp/systemd-private-ed8024f8e6534be1a2d3ad9bcda778b4-systemd-hostnamed.service
C9MX9n/tmp
/proc/sys/kernel/ngroups_max
/proc/sys/kernel/random
/proc/sys/kernel/random/boot_id
/proc/1/environ
/proc/1/status
/proc/1/comm
/proc/1/cmdline
/proc/1/exe
/proc/1/cgroup
/proc/1/loginuid
/proc/1/sessionid
/proc/347
/proc/347/cgroup
/proc/480
/proc/480/cgroup
/proc/813/net
/proc/813/mounts
/proc/816
/proc/816/status
/proc/816/comm
/proc/816/cmdline
/proc/816/exe
```

ΤΜΗΜΑ 19
ΠΡΟΣΩΡΙΝΑ ΑΠΟΘΗΚΕΥΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΣΕ ΠΡΟΓΡΑΜΜΑΤΑ ΠΕΡΙΗΓΗΣΗΣ (Διευθύνσεις, Λήψη Ιστορικού)

Συλλογή πληροφοριών από φυλλομετρητές

Όλοι οι φυλλομετρητές αποθηκεύουν πληροφορίες, όπως διευθύνσεις, ιστορικό και άλλες πληροφορίες, χρήσιμες για τον ερευνητή. Για να συλλέξουμε αυτές τις πληροφορίες, υπάρχουν αρκετά εργαλεία. Κάποια από αυτά θα τα παρουσιάσουμε στην συνέχεια.

Γενικά στην ψηφιακή σήμανση, σχετικά με τους φυλλομετρητές μπορούμε να εντοπίσουμε πληροφορίες, όπως:

- **Ποιες ιστοσελίδες επισκέφτηκε ο χρήστης**
  - History --> cache --> Cookies --> Recovery folders --> Suggested sites
- **Πόσες φορές επισκέφτηκε μία ιστοσελίδα**
  - History
- **Πότε επισκέφτηκε μία ιστοσελίδα**
  - History --> cache --> Cookies --> Recovery folders
- **Τι ιστοσελίδες αποθήκευσε ο χρήστης**
  - Bookmarks
- **Αρχεία που τυχόν κατέβασε ο χρήστης**
  - Download folder → cache
- **Εντοπισμός ονόματος χρηστών**
  - cache --> Cookies --> Recovery folders → autocomplete
- **Εντοπισμός των αναζητήσεων του χρήστη**
  - cache → autocomplete

Στην περίπτωση του Google Chrome, μπορούμε να βρούμε τα δεδομένα που αποθηκεύει ο περιηγητής στην ακόλουθη διαδρομή:

~/.cache/google-chrome/Default/Cache$

```
user2@ubuntu:~/.cache/google-chrome/Default/Cache$ ls
0259cb3766f7696d_0  415d4ae313a80640_0  7f3e625d81f23e89_0  c167fe54d77ac07a_0
0259cb3766f7696d_1  41f5a8b6ebe26801_0  7f68dcae31f06aa6_0  c167fe54d77ac07a_1
05fbbc0ba3a9ce3a_0  42c6fcaa5ee3e7ba_0  7fe8960ac3bce462_0  c45fb2a089dbc10f_0
060a055b5f8bed90_0  43bda4e0d1c3745a_0  806f05a685d7857f_0  c562ce1de5472258_0
063c27ab9d54c57e_0  4417605166039777_0  806f05a685d7857f_1  c57c1681c7d98c61_0
063c27ab9d54c57e_1  452e812858024dd5_0  8088a66adbd81bed_0  c57c1681c7d98c61_1
0640293ed3631604_0  48893015991c7b50_0  81712cf18954417e_0  c59caa8306d1f1c8_0
0640293ed3631604_1  48b9826614437c68_0  8203fdf79aff2c13_0  c6cc23107ba8761b_0
066bcf680c2f71a8_0  494b75c9faba61c7_0  8229e55cc07c69e9_0  c6cc23107ba8761b_1
07a751208f4b645f_0  494b75c9faba61c7_1  82a45794fdd7bda4_0  c80fd392bbdb5f13_0
09ae2175120bac96_0  49c87bf6402ea22a_0  8569ae7c6b781fce_0  c8384426ea96ec1b_0
0b0693e9cf7327cf_0  49c87bf6402ea22a_1  883205f2bd37b656_0  c844d238f6105b58_0
0b27f0704a5e6146_0  4ab269cbdf864932_0  8b62769bab1dc50f_0  c93faab51c27531a_0
0b58cb6d0696a23f_0  4b708aa6fca448c3_0  8b83499dc7fc2e1d_0  ca411d429765e37d_0
0b6b7b3d72a03ad3_0  4bf2fc414fbc0e58_0  8c3bfb583fb84cd5_0  ca411d429765e37d_1
0bf9ce1e4bc1325b_0  4c416703e0ceb5b6_0  8c3bfb583fb84cd5_1  cac191c57972b030_0
0dbb8db999c51b56_0  4c4bfd00269cb5ac_0  8c3d496e10fab9b9_0  cb2982c6ecb74b22_0
0e085a608757f4da_0  4c4bfd00269cb5ac_1  8ca2c7487d5be99c_0  cb57146bc41058cb_0
0e085a608757f4da_1  4e7dd10f2bf24eca_0  8d8afc16237cc9ce_0  cd29829f89ad2e42_0
```

Στην περίπτωση του Mozilla Firefox, μπορούμε να βρούμε τα δεδομένα που αποθηκεύει ο περιηγητής στην ακόλουθη διαδρομή:

~/.mozilla/firefox/

```
user2@ubuntu:~/.mozilla/firefox/6zv9zst4.default$ ls
addons.json              kinto.sqlite
addonStartup.json.lz4    minidumps
AlternateServices.txt    permissions.sqlite
blocklists               places.sqlite
blocklist.xml            prefs.js
bookmarkbackups          revocations.txt
browser-extension-data   saved-telemetry-pings
cert8.db                 search.json.mozlz4
compatibility.ini        secmod.db
containers.json          SecurityPreloadState.txt
content-prefs.sqlite     sessionCheckpoints.json
cookies.sqlite           sessionstore-backups
crashes                  sessionstore.jsonlz4
datareporting            shield-preference-experiments.json
extensions.json          SiteSecurityServiceState.txt
favicons.sqlite          storage
gmp                      storage.sqlite
gmp-gmpopenh264          times.json
handlers.json            webappsstore.sqlite
key3.db                  xulstore.json
user2@ubuntu:~/.mozilla/firefox/6zv9zst4.default$
```

Ιστορικό αναζήτησης στο Διαδίκτυο

Το ιστορικό αναζήτησης στο Διαδίκτυο αποτελεί σημαντική πληροφορία σε ορισμένα περιστατικά, κυρίως εκείνα που σχετίζονται με κάποιο είδος μόλυνσης από ιομορφικό λογισμικό που προκλήθηκε από την περιήγηση σε μολυσμένες ιστοσελίδες. Τον τελευταίο καιρό, οι δημιουργοί ιομορφικού λογισμικού έχουν εντείνει την εκμετάλλευση των τρωτοτήτων στα προγράμματα περιήγησης (και στα προγράμματα που καλούνται μέσω αυτών), στις τεχνολογίες που αναπτύσσουν ιστοσελίδες ή στους διακομιστές (servers), για να μολύνουν όσο το δυνατόν περισσότερους χρήστες. Γι' αυτό σε πολλές περιπτώσεις επιβάλλεται να ανακτήσουμε πληροφορίες σχετικά με το ιστορικό αναζήτησης, για να είμαστε σε θέση να εντοπίσουμε τη δραστηριότητα του χρήστη στο διαδίκτυο.

Cookies

Τα cookies είναι μικρά αρχεία κειμένου που επιτρέπουν, μεταξύ άλλων, να διατηρείται ανοικτή μια σύνοδος (session) σε μια ιστοσελίδα, να παρακολουθείται, να αποθηκεύονται οι προτιμήσεις, κλπ. Γενικά τα cookies είναι σημαντικά στην ανάλυση για τον καθορισμό του τρόπου χρήσης του διαδικτύου. Τα Cookies είναι μικρά text αρχεία (<4KB), τα οποία μπορούν να δώσουν στον ερευνητή τις πληροφορίες, όπως:

- Σε ποια ιστοσελίδα αναφέρονται, εφαρμόζονται
- Πληροφορίες για τον τοπικό λογαριασμό χρήστη (Local user account)
- MAC times για το αρχείο cookie
- Και ότι άλλο δεδομένο περιλαμβάνουν σχετικά με την ιστοσελίδα.

Αποθηκεύονται μόνο τα persistent cookies. Πολύ δύσκολο να αποκρυπτογραφήσουμε τα cookies.

Υπάρχουν διάφορα εργαλεία που μπορούν να χρησιμοποιηθούν ανάλογα με το πρόγραμμα περιήγησης (browser), για να δούμε τα cookies με ένα απλούστερο τρόπο.

ΤΜΗΜΑ 20
ΣΥΛΛΟΓΗ ΣΤΑΤΙΚΩΝ – ΑΠΟΘΗΚΕΥΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ (NON VOLATILE INFORMATION)

Μόλις συλλεχθούν οι πληροφορίες που μεταβάλλονται (πτητικές), είτε σε συνάρτηση με το χρόνο, είτε με την ενέργεια του χρήστη, είτε με την εκκίνηση του υπολογιστή, επόμενο βήμα είναι να συλλεχθούν οι πληροφορίες που δεν μεταβάλλονται, αλλά είναι αποθηκευμένες και μπορούν να ληφθούν ενώ ο υπολογιστής είναι εκτός λειτουργίας. Στα αποθηκευτικά μέσα (όπως σκληρός δίσκος), ο ερευνητής μπορεί να εντοπίσει πολλά και ενδιαφέροντα αποδεικτικά στοιχεία. Συνεπώς είναι σημαντική ενέργεια η δημιουργία αντιγράφου όλων των αποθηκευτικών μέσων που υπάρχουν στο υπό εξέταση σύστημα.

Όταν ερευνούμε μία συγκεκριμένη υπόθεση, ο ερευνητής θα βρεθεί σε μία από τις δύο καταστάσεις:

- Ο υπολογιστής βρίσκεται σε λειτουργία, με:
  - τα αποθηκευτικά μέσα να **μην είναι** κρυπτογραφημένα.
  - τα αποθηκευτικά μέσα να **είναι** κρυπτογραφημένα.
- Ο υπολογιστής δεν βρίσκεται σε λειτουργία.

Όταν ο υπολογιστής δεν βρίσκεται σε λειτουργία, απλά ο ερευνητής αντιγράφει τα αποθηκευτικά μέσα, δημιουργεί αντίγραφα και εργάζεται πάνω σε αυτά.

Όταν ο υπολογιστής βρίσκεται σε λειτουργία, ο ερευνητής συλλέγει τα μεταβαλλόμενα δεδομένα και στην συνέχεια εξετάζει αν τα αποθηκευτικά μέσα είναι κρυπτογραφημένα. Εάν δεν είναι κρυπτογραφημένα, σταματά την λειτουργία του υπολογιστή, αντιγράφει τα αποθηκευτικά μέσα, δημιουργεί αντίγραφα και εργάζεται πάνω σε αυτά.

Εάν τα αποθηκευτικά μέσα (σκληρός δίσκος) είναι κρυπτογραφημένα, τότε δεν σταματά την λειτουργία του υπολογιστή και κάνει αντιγραφή του σκληρού (λογικό αντίγραφο) ενώ ο υπολογιστής είναι σε λειτουργία και στην συνέχεια δημιουργεί αντίγραφα και εργάζεται πάνω σε αυτά.

Συνεπώς μπορούμε να αντιγράψουμε τα αποθηκευτικά μέσα με τρεις τρόπους:

- **Φυσικό αντίγραφο**
  - Πρόκειται για αντιγραφή bit to bit ενός σκληρού δίσκου, ενώ ο υπολογιστής είναι εκτός λειτουργίας.
- **Λογικό αντίγραφο**
  - Πρόκειται για αντιγραφή ενός σκληρού ενώ είναι σε λειτουργία ο υπολογιστής.
- **Συλλογή συγκεκριμένων - επιλεγμένων δεδομένων**, ανάλογα με την υπόθεση, στην περίπτωση που ο όγκος των αποθηκευτικών μέσων είναι τεράστιος και δεν μπορούμε να τα αντιγράψουμε.

Ψηφιακά Σημασμένη Αναπαραγωγή των Μέσων Αποθήκευσης

Υπάρχει συγκεκριμένη διαδικασία συλλογής πληροφοριών από τον σκληρό δίσκο ενός Linux συστήματος. Η συλλογή και η διαδικασία εξαρτώνται από πολλούς παράγοντες. Αν ο σκληρός είναι κρυπτογραφημένος, συλλέγουμε τα δεδομένα ενώ ο υπολογιστής είναι σε λειτουργία, διαφορετικά αντιγράφουμε τον σκληρό με τα προγράμματα που αναφέρονται στην συνέχεια:

$ dd if=system.img of=/dev/sdc bs=4096 conv=noerror

$ dcfldd if=/dev/sdb1 of=/media/disk/test_image.dd hash=md5,sha1 hashlog=/media/disk/hashlog.txt

$ ddrescue [options] infile outfile [mapfile]

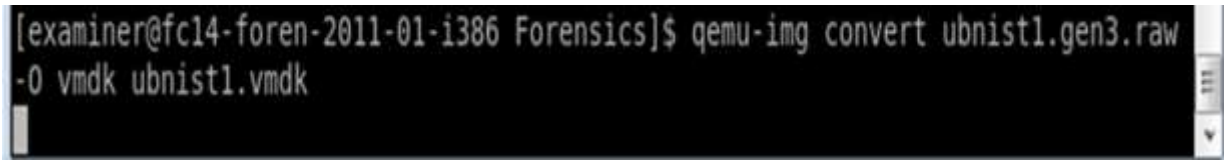
Από τη στιγμή που έχουμε την εικόνα (image) με το dd για να προβούμε στην

εξέταση του, θα το μετατρέψουμε σε ένα αρχείο της μορφής .vmdk με σκοπό να το ανοίξουμε με λογισμικό virtualization (virtualbox, vmware). Για την μετατροπή χρησιμοποιούμε το εργαλείο qemu-img (https://wiki.qemu.org/Main_Page). Στο ubuntu το εγκαθιστούμε με την εντολή:

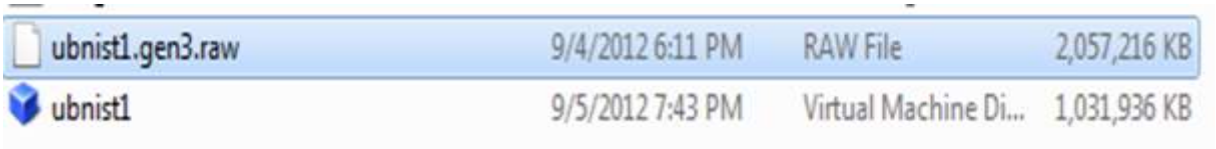
$ sudo apt-get install qemu-utils

Για την μετατροπή του σε .vmdk image χρησιμοποιώ την εντολή convert όπως παρακάτω:
$ qemu-img convert <input_file> -O <output_format> <output_filename>

$ qemu-img convert ddImage -O vmdk vmDisk



Μετά από αρκετή ώρα θα έχει παραχθεί το αρχείο που θέλουμε



Η διαδικασία συνεχίζεται με άνοιγμα του VMware Player και την επιλογή Create a new VM. Επιλέγουμε λειτουργικό σύστημα αντίστοιχο με αυτό του dd image. Δίνουμε στην μηχανή το ίδιο όνομα με τον vmdk σκληρό που δημιουργήσαμε. Η επιλογή δίσκου δεν χρειάζεται να είναι αρκετά μεγαλύτερος από τον αυθεντικό δίνοντας προσοχή στην αποθήκευση του εικονικού σκληρού ως ένα συμπαγές αρχείο. Ακολούθως αντικαθιστούμε τον εικονικό δίσκο που φτιάξαμε με αυτόν που έχουμε δημιουργήσει με το εργαλείο qemu-img και εκκινούμε την εικονική μηχανή. Με αυτόν τον τρόπο μπορούμε να ερευνήσουμε τον σκληρό δίσκο. Εναλλακτικές μέθοδοι μετατροπής είναι οι παρακάτω:

- LiveView - http://liveview.sourceforge.net/
- raw2vmdk - https://github.com/Zapotek/raw2vmdk
- ***vboxmanage convertfromraw C:\rawimage.dd C:\raw-virtual.vdi***

Εξέταση Ρυθμίσεων Ασφαλείας Συστήματος

Ευπάθειες ασφάλειας μπορούν να μας αποκαλύψουν τον τρόπο που το ιομορφικό λογισμικό τοποθετήθηκε στο παραβιασμένο μηχάνημα. Στον ιστότοπο **https://learn.cisecurity.org/benchmarks** θα βρούμε έναν αναλυτικό οδηγό για την αξιολόγηση του επιπέδου ασφάλειας ενός συστήματος Linux.

Σχέσεις των Έμπιστων Hosts

Συνδέσεις με έμπιστους hosts περιέχουν κινδύνους και μπορούν να χρησιμοποιηθούν από τον κακόβουλο για την απόκτηση πρόσβασης. Για παράδειγμα, ιομορφικό λογισμικό μπορεί να διαδοθεί από μηχάνημα σε μηχάνημα μέσω κοινόχρηστων λογαριασμών ή συστήματα στόχους που υπάρχουν στον φάκελο /etc/hosts του παραβιασμένου μηχανήματος. Επίσης, η αλλαγή ρυθμίσεων του παραβιασμένου μηχανήματος ενδέχεται να επιτρέψει συνδέσεις από μη έμπιστους hosts, όπως βάζοντας το '+' σε εγγραφές και μη έμπιστα ονόματα στα αρχεία /etc/hosts.equiv ή /etc/hosts.lpd

Ανάκτηση Αρχείων Καταγραφής Συστήματος

Αναλύοντας τα αρχεία καταγραφής μπορούμε να ανακτήσουμε πολύτιμα δεδομένα σχετικά με το περιστατικό που περιέχουν χρονικά πλαίσια (timeframes), διευθύνσεις IP, άγνωστους λογαριασμούς χρηστών και εγκατεστημένα rootkits και κακόβουλες υπηρεσίες. εντοπίσουμε την δραστηριότητα ενός κακόβουλου χρήστη. Υπάρχουν πολλά μητρώα καταγραφής συμβάντων σε ένα μηχάνημα linux, όπως τα "wtmp" , "lastlog" και "utmp". Με την εντολή last μπορώ να δω τις προσπάθειες εισόδου στο υπό εξέταση σύστημα:

$: last

Στη διαδρομή "/var/log " ή στο "/var/adm." εντοπίζουμε τα μητρώα καταγραφής συμβάντων σε *nix λειτουργικά συστήματα. Οι ρυθμίσεις εντοπίζονται στο "/etc/syslog.conf" αρχείο.

Αναλυτικά τι αποθηκεύει το κάθε αρχείο καταγραφής φαίνεται στην παρακάτω λίστα:

/var/log/messages – Περιέχει μηνύματα συστήματος που καταγράφονται κατά την εκκίνηση του συστήματος. Υπάρχουν πολλά δεδομένα που αποθηκεύονται όπως mail, cron, daemon, kern, auth, etc.
/var/log/dmesg – Περιέχει πληροφορίες σχετικά με το buffer του πυρήνα. Όταν το σύστημα εκκινεί, εκτυπώνει αριθμό μηνυμάτων στην οθόνη που εμφανίζει πληροφορίες σχετικά με τις συσκευές υλικού που εντοπίζει ο πυρήνας κατά τη διαδικασία εκκίνησης. Αυτά τα μηνύματα είναι διαθέσιμα στο buffer του πυρήνα και κάθε φορά το νεότερο μήνυμα διαγράφει το παλαιότερο. Μπορούμε να προβάλουμε το περιεχόμενο αυτού του αρχείου χρησιμοποιώντας την εντολή dmesg.
/var/log/auth.log – Περιέχει πληροφορίες συστήματος σχετικές με τις συνδέσεις των χρηστών και των μηχανισμών αυθεντικοποίησης που χρησιμοποιήθηκαν.
/var/log/boot.log – Περιέχει πληροφορίες που καταγράφονται όταν το σύστημα βρίσκεται στην φάση της εκκίνησης.
/var/log/daemon.log – Περιέχει πληροφορίες που καταγράφονται από τις

διάφορες διεργασίες παρασκηνίου (daemons)[12] που εκτελούνται στο σύστημα.
/var/log/dpkg.log – Περιέχει πληροφορίες που καταγράφονται όταν ένα πακέτο (package) εγκαθίσταται ή απεγκαθίσταται με την εντολή dpkg.
/var/log/kern.log – Περιέχει πληροφορίες που καταγράφονται από τον πυρήνα. Είναι ιδιαίτερα χρήσιμη για την επίλυση προβλημάτων πυρήνες που είναι custom-built.
/var/log/lastlog – Εμφανίζει τις πρόσφατες πληροφορίες σύνδεσης για όλους τους χρήστες. Αυτό δεν είναι ένα αρχείο ascii. Θα πρέπει να χρησιμοποιήσετε την εντολή lastlog για να δείτε το περιεχόμενο αυτού του αρχείου.
/var/log/maillog, /var/log/mail.log – Περιέχει τις πληροφορίες καταγραφής από τον διακομιστή αλληλογραφίας που εκτελείται στο σύστημα. Για παράδειγμα, το sendmail καταγράφει πληροφορίες σχετικά με όλα τα απεσταλμένα αντικείμενα σε αυτό το αρχείο.
/var/log/user.log – Περιέχει τις πληροφορίες σχετικά με τα αρχεία καταγραφής επιπέδου χρήστη.
/var/log/Xorg.x.log – Καταγράφει μηνύματα από το X
/var/log/alternatives.log – Οι πληροφορίες από το update-alternatives καταγράφονται σε αυτό το αρχείο. Στο Ubuntu τα update-alternatives διατηρούν συμβολικούς συνδέσμους (symbolic links) που καθορίζουν προεπιλεγμένες εντολές.
/var/log/btmp – Αυτό το αρχείο περιέχει πληροφορίες σχετικά με αποτυχημένες προσπάθειες σύνδεσης. Χρησιμοποιήστε την εντολή last για να προβάλουμε το αρχείο btmp. Για παράδειγμα, **"last -f / var/log/btmp | more**"
/var/log/cups – Όλα τα μηνύματα σχετικά με τους εκτυπωτές και τις εργασίες εκτύπωσης
/var/log/anaconda.log – Όταν εγκαθίσταται το Linux, όλα τα μηνύματα που σχετίζονται με την εγκατάσταση αποθηκεύονται σε αυτό το αρχείο καταγραφής.
/var/log/yum.log – Περιέχει πληροφορίες που καταγράφονται όταν ένα πακέτο είναι εγκαθίσταται με την χρήση του yum.
/var/log/cron – Κάθε φορά που ένας cron daemon (ή anacron) ξεκινά μια εργασία cron, καταγράφει τις πληροφορίες σχετικά με την εργασία cron σε αυτό το αρχείο.
/var/log/secure – Περιέχει πληροφορίες σχετικά με τα δικαιώματα αυθεντικοποίησης και εξουσιοδότησης. Για παράδειγμα, το sshd καταγράφει όλα τα μηνύματα εδώ, συμπεριλαμβανομένων των ανεπιτυχών σύνδεσεων.
/var/log/wtmp or /var/log/utmp – Περιέχει καταγραφές των αρχείων σύνδεσης. Χρησιμοποιώντας το wtmp μπορείτε να μάθετε ποιος συνδεθεί στο σύστημα. Η εντολή who χρησιμοποιεί αυτό το αρχείο.
/var/log/faillog – Περιέχει αποτυχημένες προσπάθειες σύνδεσης χρήστών. Χρησιμοποιήστε την εντολή faillog για να εμφανίσετε το περιεχόμενο αυτού του αρχείου.
/var/log/httpd/ (or) /var/log/apache2 – Περιέχει τα αρχεία access_log και error_log του διακομιστή διαδικτύου apache
/var/log/lighttpd/ – Περιέχει τα αρχεία access_log και error_log του διακομιστή light HTTPD.
/var/log/mail/ – Αυτός ο υποκατάλογος (subdirectory) περιέχει πρόσθετα αρχεία καταγραφής από τον διακομιστή αλληλογραφίας. Για παράδειγμα, το sendmail αποθηκεύει τα στατιστικά στοιχεία συλλογής αλληλογραφίας στο αρχείο

[12] Ένας daemon είναι μία διεργασία παρασκηνίου που χειρίζεται τις αιτήσεις για υπηρεσίες όπως εκτύπωση και μεταφορά αρχείων και είναι αδρανής όταν δεν απαιτείται.

/var/log/mail/statistics

/var/log/prelink/ – το πρόγραμμα prelink τροποποιεί τις κοινές βιβλιοθήκες και τα συνδεδεμένα δυαδικά αρχεία για να επιταχύνουν τη διαδικασία εκκίνησης. Το /var/log/prelink/prelink.log περιέχει πληροφορίες σχετικά με το αρχείο .so που τροποποιήθηκε από το prelink

/var/log/audit/ – Περιέχει πληροφορίες καταγραφής που αποθηκεύονται από τον daemon auditd.

/var/log/setroubleshoot/ – Το SELinux χρησιμοποιεί το setroubleshootd (SE Trouble Shoot Daemon) για να ειδοποιεί για θέματα που αφορούν το περιβάλλον ασφαλείας των αρχείων και καταγράφει αυτές τις πληροφορίες σε αυτό το αρχείο.

/var/log/samba/ – Περιέχει πληροφορίες καταγραφής αποθηκευμένες από το samba, το οποίο χρησιμοποιείται για τη σύνδεση των Windows με το Linux.

/var/log/sa/ – Περιέχει τα καθημερινά αρχεία sar που συλλέγονται από το πακέτο sysstat.

/var/log/sssd/ – Χρησιμοποιείται από δαίμονες υπηρεσιών ασφαλείας συστημάτων που διαχειρίζονται την πρόσβαση σε απομακρυσμένους καταλόγους και μηχανισμούς αυθεντικοποίησης.

$ grep -c sudo /var/log/auth.log
$ grep -i sudo /var/log/auth.log
$ grep -i trixd00r /var/log/syslog
$ grep -i Accepted /var/log/auth.log
$ grep -i Failed /var/log/auth.log
$ zcat file.gz | grep -i Accepted
$ zcat syslog.*.gz | grep -i adore
$ zcat auth.log.*.gz | grep -i accepted
$ zcat auth.log.*.gz | grep -i -A 5 accepted
$ zcat auth.log.*.gz | grep -i -A 5 -B 5 accepted
$ zcat auth.log.*.gz | grep -i failed
$ echo "There were $(grep -c ' sudo: ' /var/log/auth.log) attempts to use sudo, $(grep -c ' sudo: .*authentication failure' /var/log/auth.log) of which failed."
$ echo "There were $(grep -c ' Accepted ' /var/log/auth.log) attempts to connect, $(grep -c ' Failed' /var/log/auth.log) of which failed."

- **Αποκατάσταση διαγραμμένων αρχείων**

Υπάρχουν εργαλεία που μπορούν να μας βοηθήσουν να αποκαταστήσουμε διεγραμμένα αρχεία, όπως το foremost και τα ακόλουθα:

Testdisk	http://www.cgsecurity.org/wiki/TestDisk
extundelete	http://extundelete.sourceforge.net

Εξαγωγή Ιομορφικού Λογισμικού

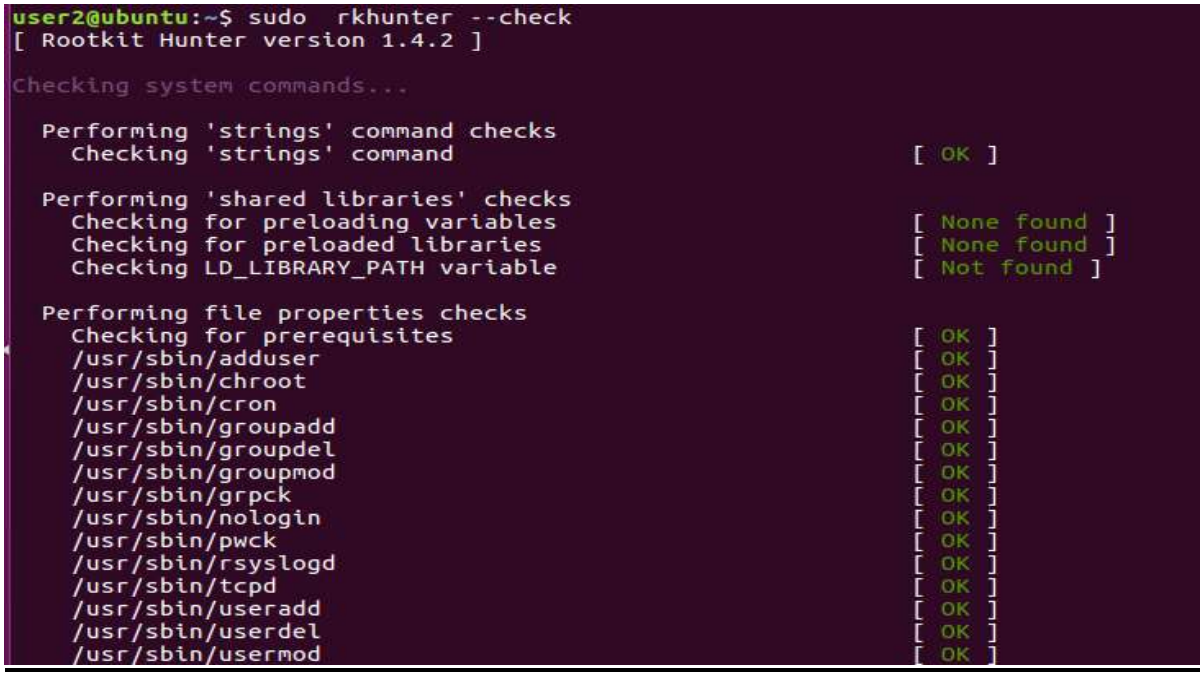
Για να διαπιστώσουμε αν υπάρχει εγκατεστημένο γνωστό ιομορφικό λογισμικό μπορούμε να εγκαταστήσουμε τα προγράμματα rkhunter και chkrootkit τα οποία εκτελούν εκτεταμένους ελέγχους.

Εγκατάσταση σε Ubuntu:

 # apt-get install rkhunter chkrootkit

 # chkrootkit

 # rkhunter - - check



ΤΜΗΜΑ 21
ΕΛΕΓΧΟΣ ΑΚΕΡΑΙΟΤΗΤΑΣ ΔΕΔΟΜΕΝΩΝ

./.

Κατά την διαδικασία της συλλογής δεδομένων όπως είδαμε θα χρειαστεί να εκτελέσουμε έλεγχο ακεραιότητας δεδομένων σε διάφορες φάσεις είτε για να επιβεβαιώσουμε ότι μία εικόνα (image) μνήμης δεν έχει τροποποιηθεί, είτε να διαπιστώσουμε αν κάποιος έχει αλλάξει τα δεδομένα με κάποια άλλα τα οποία έχουν ιομορφικό κώδικα. Στον έλεγχο ακεραιότητας συγκρίνω μέσω ειδικών εργαλείων δύο ή περισσότερα αρχεία. Αν τα αρχεία είναι πανομοιότυπα τότε αλγόριθμος κατακερματισμού του εργαλείου θα επιστρέψει ακριβώς το ίδιο αποτέλεσμα με τη μορφή ακολουθίας γραμμάτων και αριθμών. Αντιθέτως, αν τα αρχεία διαφέρουν έστω και κατά ένα bit πληροφορίας, το αποτέλεσμα θα είναι τελείως διαφορετικό. Για τον έλεγχο ακεραιότητας χρησιμοποιούμε διάφορους αλγόριθμους όπως MD5, SHA-1, SHA-2, κλπ.

Η χρήση του MD5 hash, παρά την τεράστια χρήση του, παρουσιάζει το πρόβλημα της σύγκρουσης τιμών, με άλλα λόγια, θα μπορούσε να συμβεί διαφορετικά αρχεία να έχουν το ίδιο MD5, πράγμα που σημαίνει ότι η εγκυρότητα της απόδειξής του θα μπορούσε να αμφισβητηθεί. Γι' αυτό συνιστάται η μείωση της χρήσης του.

Μια παρόμοια περίπτωση, μολονότι δεν είναι πανομοιότυπη, είναι το SHA-1, γι' αυτό καλό είναι να αναζητήσουμε διάφορες εναλλακτικές λύσεις, όπως τα SHA-256, SHA-512, κλπ.

Υπάρχει αριθμός εργαλείων τα οποία μπορούν να βοηθήσουν στην δημιουργία διαφορετικών τιμών hashes για ένα αρχείο. Ένα παράδειγμα της χρήσης του sha256sum φαίνεται παρακάτω:

```
user2@ubuntu:~$ sha256sum examples.desktop
913b87897ffb6dca07e9f17e280aa8ecb9886dffeda8a15efeafec11dec0d108  examples.deskt
op
user2@ubuntu:~$
```

ΚΕΦΑΛΑΙΟ ΣΤ
ΑΝΑΣΚΟΠΗΣΗ

ΤΜΗΜΑ 22
ΕΠΙΛΟΓΟΣ

Όπως επισημάνθηκε στην αρχή του εγχειριδίου, η έννοια της ψηφιακής εγκληματολογικής ανάλυσης, αναφέρεται στο συνδυασμό των διαδικασιών συλλογής πληροφοριών και ανάλυσης αποδεικτικών στοιχείων που πραγματοποιούνται με σκοπό την αντιμετώπιση ενός περιστατικού που σχετίζεται με την ασφάλεια ενός υπολογιστή και, σε ορισμένες περιπτώσεις, μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία στο δικαστήριο. Μέσω αυτής της διαδικασίας, ο στόχος είναι να απαντηθούν τα ακόλουθα ερωτήματα: **Τι; Πού; Πότε; Γιατί; Ποιος; Πώς;**

Η επιστήμη αυτή λαμβάνει ένα πολύ σημαντικό ρόλο τα τελευταία χρόνια και η χρήση της επεκτείνεται, καθώς είναι συχνά τα περιστατικά που σχετίζονται με την ασφάλεια υπολογιστών, όπως παραβιάσεις συστημάτων, υποκλοπή πληροφοριών, μολύνσεις με ιούς, κλπ.

Υπάρχουν διαφορετικές μεθοδολογίες που μπορούν να υιοθετηθούν για τη ολοκλήρωση αυτής της διαδικασίας, που είναι όλες βασισμένες στην ίδια γενική ιδέα και έχουν κοινές κατευθυντήριες γραμμές και φάσεις. Μία από τις πιο σημαντικές, είναι αυτή που περιγράφεται και αναφέρεται λεπτομερώς στο έγγραφο *RFC3227*. Μεταξύ των πιο σημαντικών πτυχών που πρέπει να έχουμε κατά νου και για την οποία το *RFC3227* κάνει ειδική μνεία, είναι η σειρά της μεταβλητότητας των αποδεικτικών στοιχείων, που δείχνει ότι το πρώτο καθήκον είναι να ανακτηθούν τα αποδεικτικά στοιχεία που θα είναι διαθέσιμα μόνο για περιορισμένο χρονικό διάστημα και στην συνέχεια τα υπόλοιπα .

Σε γενικές γραμμές, λαμβάνουμε ένα αντίγραφο της μνήμης και του σκληρού δίσκου και τα αναπαράγουμε προκειμένου να εργαστούμε πάνω στα αντίγραφα, για τη λήψη των περαιτέρω αποδεικτικών στοιχείων. Ωστόσο, κατά τη διεξαγωγή της διαδικασίας, είναι πολύ σημαντικό να έχουμε σαφή ιδέα για το συγκεκριμένο τύπο του περιστατικού, προκειμένου να εξακριβώσουμε ποιες πληροφορίες πρέπει να συλλεχθούν και πώς θα προχωρήσουμε.

Τέλος, αξίζει να υπογραμμιστεί ότι κάθε διαδικασία πρέπει να πραγματοποιείται με ένα πολύ αυστηρό και σχολαστικό τρόπο, με σκοπό τη διατήρηση της ακεραιότητας και της εγκυρότητάς της.

ΥΠΟΔΕΙΓΜΑΤΑ

(Υπόδειγμα 1)

ΣΥΣΤΗΜΑΤΑ ΠΟΥ ΕΜΠΛΕΚΟΝΤΑΙ ΣΤΟ ΠΕΡΙΣΤΑΤΙΚΟ

Α/Α	ΣΥΣΤΗΜΑ	ΜΠΟΡΕΙ ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΘΕΙ ΓΙΑ ΕΞΑΓΩΓΗ ΣΤΟΙΧΕΙΩΝ	ΠΑΡΑΤΗΡΗΣΕΙΣ

(Υπόδειγμα 2)
ΛΙΣΤΑ ΕΝΕΡΓΕΙΩΝ

A/A			
Πτητικά Δεδομένα			
1	**Ανάκτηση Φυσικής Μνήμης**		
2	**Καταγραφή Λεπτομερειών Συστήματος**		
3	**Συνδεδεμένοι Χρήστες στο Σύστημα**		
4	**Συνδέσεις και Δραστηριότητα Δικτύου**		
5	**Τρέχουσες Διεργασίες**		
6	**Συσχέτιση Θυρών και Διεργασιών**		
7	**Εντοπισμός ΄Υποπτων Υπηρεσιών**		
8	**Ανάκτηση Ενοτήτων Πυρήνα (Kernel Modules)**		
9	**Εντοπισμός ανοικτών αρχείων**		
10	**Ανάκτηση Ιστορικού Εντολών**		
11	**Επιθεώρηση Κοινοχρήστων Δικτύου (Network Shares)**		
12	**Εξέταση Προγραμματισμένων Εργασιών**		
13	**Εξέταση Περιεχομένων Πρόχειρου (Clipboard)**		
14	**Εντοπισμός των αρχείων setuid και setgid**		
Μη Πτητικά Δεδομένα			
1	**Ψηφιακά Σημασμένη Αναπαραγωγή των Μέσων Αποθήκευσης**		
2	**Εξέταση Ρυθμίσεων Ασφαλείας Συστήματος**		
3	**Σχέσεις των ΄Εμπιστων Hosts**		
4	**Εντοπισμός Μηχανισμών Επιμονής (Persistence Mechanisms)**		
5	**Ανάκτηση Αρχείων Καταγραφής Συστήματος**		
6	**Πληροφορίες της Πολιτικής Χρηστών και Ομάδων**		
7	**Εντοπισμός ΄Υποπτων Κρυφών Αρχείων**		
8	**Δραστηριότητες Περιήγησης στο Διαδίκτυο**		
Εξαγωγή Ιομορφικού Λογισμικού			
1	**Εντοπισμός και Εξαγωγή ΄Υποπτων Αρχείων**		

(Υπόδειγμα 3)
ΑΛΥΣΙΔΑ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

Ποιοι ήταν στο χώρο;

Τι έκαναν;

Τι έψαχναν;

Πως αντέδρασαν;

Ποιος ανακάλυψε και συγκέντρωσε τα αποδεικτικά στοιχεία;

Πότε ;

Που;

Ποιος χειρίστηκε τα αποδεικτικά στοιχεία;

Πότε ;

Που;

Ποιος φύλαγε τα αποδεικτικά στοιχεία;

Για πόσο καιρό;

Πώς τα αποθήκευε;

Εάν τα αποδεικτικά στοιχεία άλλαξαν επιμέλεια / χέρια φύλαξης/παρακολούθησης, πότε και πώς έλαβε χώρα η ανταλλαγή (συμπεριλαμβανομένου του αριθμού δελτίου παράδοσης, κλπ);

Αριθμός Υπόθεσης:

Είδος Περιστατικού:

Επηρεαζόμενη Υπηρεσία:

Διεύθυνση:

Τηλέφωνο:

Ημερομηνία και Ώρα:

Ερευνητής:

Παρατηρήσεις;

(Υπόδειγμα 4)

ΕΠΑΦΕΣ

ΛΙΣΤΑ ΕΠΑΦΩΝ
Αριθμός Υπόθεσης:
Αριθμός σελίδας:

Ονοματεπώνυμο	Email	Τηλέφωνο	Θέση

Αριθμός Υπόθεσης:

Είδος Περιστατικού:

Επηρεαζόμενη Υπηρεσία:

Διεύθυνση:

Τηλέφωνο:

Ημερομηνία και Ώρα:

Ερευνητής:

Παρατηρήσεις;

(Υπόδειγμα 5)

ΛΙΣΤΑ ΑΠΟΔΕΙΞΕΩΝ

Αριθμός Υπόθεσης:
Αριθμός σελίδας:

Αποδεικτικό Στοιχείο	Ποσότητα	Περιγραφή αντικειμένου (Μάρκα, μοντέλο, σειριακός αριθμός, κατάσταση, κ.τ.λ.)