Network Forensics

Τι ειναι η δικανικη υπολογιστων (Computer Forensics)?

- Η Δικανικη Υπολογιστων περιλαμβανει την διατηρηση, ταυτοποιηση εξαγωγη, τεκμηριωση και διερμηνευση των υπολογιστικων μεσων για ευρεση αποδεικτικων στοιχειων η/και αναλυση των αιτιων του συμβαντος.
- Ανεκυψε ως αποτελεσμα του διαρκως αυξανομενου προβληματος του ηλεκτρονικου εγκληματος (computer crime)
- Το ηλεκτρονικο εγκλημα διακρινεται σε δυο κατηγοριες:
  - Ο υπολογιστης είναι ένα εργαλείο που χρησιμοποιείται σε ένα εγκλημα.
    - Η διερευνηση αυτων των εγκληματων συχνα περιλαμβανει την αναζητηση των υπολογιστων που εμπλεκονται στο εγκλημα.
  - Ο ιδιος ο υπολογιστης είναι το θυμα ενός εγκληματος. Αυτό συχνα αναφερεται ως αντιμετωπιση περιστατικων (incident response).
    - Αναφερεται στην εξεταση των συστηματων που εχουν δεχτει επιθεση εκ του μακροθεν (remotely attacked).
- Οι ειδικοι της δικανικης ακολουθουν ξεκαθαρες και καλα ορισμενες διαδικασιες

- Η δικανικη υπολογιστων ξεκινησε λιγα χρονια πριν, όταν ηταν απλο να συλλεχθουν αποδεικτικα στοιχεια απο έναν υπολογιστη.
- Ενω οι βασικες μεθοδολογιες της δικανικης παραμενουν οι ιδιες, η τεχνολογια αλλαζει γρηγορα και αυτό είναι μια προκληση για τους ειδικους της δικανικης.
- Η βασικη μεθοδολογια της δικανικης αποτελειται από τα εξης στοιχεια:
  - Αποκτηση των αποδεικτικων στοιχειων χωρις την καταστροφη των αυθεντικων
  - Πιστοποιηση ότι τα αποκτηθεντα στοιχεια είναι τα ιδια με τα αυθεντικα στοιχεια
  - Αναλυση των δεδομενων χωρις αυτά να τροποποιηθουν

Αποκτηση των στοιχειων

- Πρεπει να εχουμε κατά νουν ότι κάθε περιπτωση είναι διαφορετικη
- Δεν πρεπει να αποσυνδεουμε τους υπολογιστες γιατι τα αποδεικτικα στοιχεια μπορει να βρισκονται μονο στη μνημη. Αρα πρεπει να συλλεγουμε στοιχεια από το «ζωντανο συστημα» (live system).
- Δυο σημαντικα σημεια:
  - Ο χειρισμος των αποδεικτικων στοιχειων- αν δεν φροντισουμε για τα στοιχεια, το υπολοιπο της διερευνησης θα υπονομευτει
  - Αλυσιδα φυλαξης (Chain of custody) – ο στοχος της διατηρησης μια καλης αλυσιδας φυλαξης ειναι να εξασφαλιζουμε την ακεραιοτητα των αποδεικτικων στοιχειων και να αποτρεψουμε της αλλοιωση τους. Η αλυσιδα πρεπει να απανταει στα εξης ερωτηματα:
    - Ποιος τα συνελλεξε
    - Πως και που
    - Ποιος τα κατειχε
    - Πως αποθηκευτηκαν και προστατευτηκαν κατά την αποθηκευση τους
    - Ποιος τα εξηγαγε από την αποθηκευση και γιατι

- Συλλογη
  - Θελουμε οι αποδειξεις να είναι τοσο ξεκαθαρες ωστε να υποστηριζουν την υποθεση
- Ταυτοποιηση
  - Μεθοδικα ταυτοποιησε και βαλε ετικετα σε κάθε στοιχειο που εξαγεται απο την τοποθεσια του θυματος ή του υποπτου
- Μεταφορα
  - Οι αποδειξεις γενικα δεν πρεπει να μετακινουνται, αρα όταν τις μετακινουμε πρεπει αυτό να γινεται με εξαιρετικη προσοχη
- Αποθηκευση
  - Διατηρησε τις αποδειξεις σε ένα δροσερο, ξηρο και καταλληλο για ηλεκτρονικες αποδειξεις μερος
- Τεκμηριωση της διερευνησης
  - Είναι το πιο δυσκολο για τους επαγγελματιες των υπολογιστων γιατι οι τεχνικοι δεν είναι καλοι στο γραψιμο λεπτομερειων των διαδικασιων

- Πιστοποιηση της αυθεντικοτητας των αποδεικτικων στοιχειων
  - Αυτο είναι δυσκολο γιατι
    - Η σκηνες των εγκληματων αλλαζουν
    - Τα αποδεικτικα στοιχεια συχνα καταστρεφονται από τις περιβαλλοντικες συνθηκες
    - Οι συσκευες των υπολογιστων αργα χειροτερευουν
  - Κρατα αποδειξεις της ακεραιοτητας και χρονοσφραγισε τις αποδειξεις μεσω της κρυπτογραφησης των αρχειων δεδομενων
    - Δυο αλγοριθμοι (MD5 και SHA) είναι χρησιμοποιουνται συχνα σημερα για το σκοπο αυτο
- Αναλυση
  - Κανε δυο αντιγραφα ασφαλειας (backups)
  - Χρησιμοποιησε κάθε γνωστο εργαλειο αναλυσης

Παρακολουθηση του δραστη

- Λάβετε υπόψη ότι τα λαγωνικά του κυβερνοχώρου συχνά πρέπει να παρακολουθούν τους παραβάτες
- Επισης, ότι οι ψηφιακες τεχνικες και εργαλεια δικανικης είναι ελαχιστα ανεπτυγμενα
- Παρακολουθηση διευθυνσεων IP
- Μαθετε να διαβαζετε ένα email trail.
- NetBIOS – ένα πρωτοκολλο των Windows που χρησιμοποιειται αποκλειστικα σε LANS (αντι για το TCP/IP) τωρα τρεχει πανω από TCP/IP για να καλυψει WANs, εχει μια συναρτηση *nbstat* που μπορει να απεικονισει τα στατιστικα του πρωτοκολλου για ολες τις συνδεσεις TCP/IP.
- Αλλα εργαλεια παρακολουθησης είναι τα Neotrace και Netscan Pro που μπορουν να εκτελεσουν trace route
- Χρησιμοποιησε τα αρχεια καταγραφης IDS

Μεσα αποθηκευσης

- Σκληροι δισκοι
  - Κανε μια image copy και στη συνεχεια κανε restore την image σε έναν «καθαρο» σκληρο δισκο για αναλυση
  - Ξανα-ανεβασε την κοπια και ξεκινα να την αναλυεις.
  - Πριν την ανοιξεις παρε πληροφορια για την διαμορφωση της
  - Χρησιμοποιησε εργαλεια για να δημιουργησεις μια αναφορα με λιστες του περιεχομενου του δισκου (PartitionMagic)
  - Δες τα αρχεια καταγραφης του λειτουργικου συστηματος (operating system logs).

Κρυπτογραφηση και Δικανικη

- Πολλες φορες τα αποδεικτικα στοιχεια μπορει να είναι κρυπτογραφημενα. Βρειτε έναν τροπο να τα αποκρυπτογραφησετε διατηρωντας την ακεραιοτητα τους.
- Εκτος από τους κρυπτογραφικους κωδικες και η συμπιεση των δεδομενων μπορει να καταστησει το εργο της δικανικης δυσκολο.
- Βρειτε έναν τροπο να υπερβειτε τη συμπιεση και τη χρηση κρυπτογραφικων κωδίκων.

Κρυψιμο Δεδομενων (Data Hiding)

- Υπαρχουν αρκετες τεχνικες που χρησιμοποιουν οι εισβολεις για να κρυψουν δεδομενα.
  - «Θολωμα» των δεδομενων μεσω κρυπτογραφησης και συμπιεσης.
  - Κρυψιμο μεσω κωδίκων, στεγανογραφιας, ενσωματωσης ονοματος και nonames στα αρχεια
  - «Τυφλωση» των ερευνητων μεσω της αλλαγης συμπεριφορας των εντολων συστηματος και της τροποποιησης των λειτουργικων συστηματων.
- Χρησιμοποιησε γνωστα εργαλεια για να αντιμετωπισεις τις προσπαθειες αυτες

Εχθρικος Κωδικας (Hostile Code)

- Ο κάθε μη εξουσιοδοτημενος κωδικας στον υπολογιστη. Γινεται ολοενα και πιο σημαντικος.
- Ο εχθρικος κωδικας χωριζεται σε δυο κατηγοριες:
  - **Manual** – όπως network tools που επιτρεπουν μη εξουσιοδοτημενη προσβαση (NetBus, BackOrifice, IRC), fix utilities που χωρις να γινονται αντιληπτες αντικαθιστουν τον νομιμο κωδικα με εχθρικη εκδοση , παραποιητες αρχειων καταγραφης, σαρωτες τρωσιμοτητας, DDoS,
  - **Αυτονομος** – viruses (Melissa, time bombs), DDoS, and IRC bots.

Δικανικη Ηλεκτρονικη Εργαλειοθηκη (Forensic Electronic Toolkit)

- Η δικανικη υπολογιστων και δικτυων περιλαμβανει και απαιτει:
  - Ταυτοποιηση (Identification)
  - Εξαγωγη (Extraction)
  - Διατηρηση (Preservation)
  - Τεκμηριωση (Documentation)
- Αρκετα εργαλεια χρειαζονται για να γινει αυτό ολοκληρωμενα
- Η δικανικα σωστη μεθοδος ποτε δεν περιλαμβανει εξεταση των πρωτοτυπων μεσων
- Πριν χρησιμοποιησεις οποιοδηποτε δικανικο software, βεβαιωσου ότι ξερεις πώς να το χρησιμοποιεις και επισης γνωριζεις πως δουλευει.
- Εργαλεια:
  - Hard Drive - χρησιμοποιησε partitioning και viewing (Partinfo and PartitionMagic)
  - File Viewers – για να μελετουμε στοιβες με ενοχοποιητικά ή αποδεικτικά στοιχεία (Qiuckview Plus, Conversion Plus, DataViz, ThumnsPlus)

Αλλα εργαλεια (cont.)

- Unerase – Αν τα αρχεια δεν υπαρχουν πλεον στο recycle bin ή αν η ερευνα αφορα παλιο συστημα χωρις recycle bins.
- CD-R/W – εξεταστε τα οσο το δυνατον πιο προσεκτικα. Χρησιμοποιειστε CD-R Diagnostics
- Text – επειδη τα δεδομενα σε μορφη text μπορει να είναι τεραστια σε ογκο, χρησιμοποιειστε εργαλεια για γρηγορη σαρωση όπως το dtSearch.
- Αλλα συνολα εργαλειων:
  - Forensic toolkit – command-line utilities που χρησιμοποιουνται για να ανακατασκευασουμε δραστηριοτητες προσβασης (access activities) σε συστηματα με NT File system
  - Coroner toolkit - για τη διερευνηση ενός hacked Unix host.
  - ForensiX – ένα παντος σκοπου συνολο από εργαλεια συλλογης και αναλυσης δεδομενων που τρεχουν κυριως σε Linux.
  - New Technologies Incorporated (NTI)
  - EnCase
  - Hardware- Forensic-computers.com

Δικανικη που βασιζεται σε OS Brands

- Διερευνηση
  - Windows computers – προσεξτε τη Registry. Περιεχει πλουσια πληροφορια
  - Unix – ριξτε μια ματια σε password files, shell, filesystem

Οδηγιες για την αντιμετωπιση περιστατικου σε Δεδομενα Internet

- Αποκαταστησε την υπηρεσια με ασφαλεια
- Εκτιμησε την εκταση και το κοστος του περιστατικου
- Προσδιορισε την πηγη της επιθεσης και το κινητρο των δραστων
- Αποτρεψε μελλοντικα εγκληματα
- Αποκαταστησε τις απωλειες
- Προστατεψε τη δημοσια εικονα
- Δειξε τη δεουσα επιμελεια
- Λαβε υποψη σου την εταιρικη ευθυνη
- Αυξησε την κατανοηση του τοπιου της ασφαλειας

Ρολοι και Ευθυνες

- Για να διευκολυνθει η ομαδα εργασιας οι ρολοι του οργανισμου πρεπει να ανατεθουν ως ακολουθως:
  - Ομαδα εταιρικης ασφαλειας και περιστατικων
  - Ερευνητης Ασφαλειας (Security investigator)
  - Emergency response core team
  - Ιδιοκτητης εφαρμογης (Application owner)
  - Προγραμματιστης εφαρμογης (Application developer)
  - Ιδιοκτητης/διαχειριστης εφαρμογης (System owner/administrator)
  - Διαχειριστης Δικτυου (Network administrator)
  - Διαχειριστης Firewall (Firewall administrator)
  - Συμβουλοι ασφαλειας (Security consultants)

Συνοψη

Εξετασαμε:

- Τι ειναι η δικανικη υπολογιστων
- Αποκτηση των στοιχειων
- Παρακολουθηση του δραστη
- Δικανικη και Μεσα αποθηκευσης
- Δικανικη και Κρυπτογραφηση
- Εχθρικος Κωδικας
- Δικανικη Ηλεκτρονικη Εργαλειοθηκη
- Οδηγιες για την αντιμετωπιση περιστατικου
- Ρολοι και Ευθυνες

Βιβλιογραφια

- J.Kizza, F.M.Kizza, “Securing the Information Infrastructure”, IGI Global, 2008.