ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Εγκατάσταση Honeypot και ανάλυση των αποτελεσμάτων με στόχο την εύρεση attack paths/threat profiles

Τοπάλης Απόστολος

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ
Επιβλέπων
Σταμούλης Γεώργιος

Λαμία, 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Install Honeypot and analyze results to find attack paths / threat profiles

Topalis Apostolos

Master thesis

Stamoulis George

Lamia, 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ»

Εγκατάσταση Honeypot και ανάλυση των αποτελεσμάτων με στόχο την εύρεση attack paths/threat profiles

Τοπάλης Απόστολος

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

Επιβλέπων

Σταμούλης Γεώργιος

Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία,

Υπογραφή

Εγκατάσταση Honeypot και ανάλυση των αποτελεσμάτων με στόχο την εύρεση attack paths/threat profiles

Τοπάλης Απόστολος

Τριμελής Επιτροπή:

Ονοματεπώνυμο, …..(επιβλέπων/σα)

Ονοματεπώνυμο, ……

Ονοματεπώνυμο, …….

Επιστημονικός Σύμβουλος:

Ονοματεπώνυμο…..

ΠΕΡΙΛΗΨΗ

Τα Honeypots είναι συστήματα που έχουν ως σκοπό να εξαπατήσουν κακόβουλους χρήστες που προσπαθούν να επιτεθούν σε διακομιστές καθώς και σε όλη τη δικτυακή υποδομή διαφόρων οργανισμών. Τα συστήματα αυτά χωρίζονται σε δύο κατηγορίες. Η μια κατηγορία είναι honeypots παραγωγής τα οποία είναι για την προστασία πραγματικών συστημάτων ενός οργανισμού. Και η άλλη κατηγορία είναι τα ερευνητικά honeypots τα οποία είναι καθαρά για την μελέτη και ανάλυση των επιθέσεων που προσπαθούν να κάνουν οι εκάστοτε εισβολείς.

Στα πλαίσια αυτής της Μεταπτυχιακής Διατριβής, εγκαταστάθηκε το honeydrive και παραμετροποιήθηκε έτσι ώστε να λειτουργήσει το Honeypot Kippo. Οι επιθέσεις που καταγράφηκαν αναλύθηκαν και παρουσιάστηκαν με πίνακες και γραφήματα. . Συγκεκριμένα το kippo honeypot παίζει τον ρόλο μιας διαδικτυακής παγίδας έτσι ώστε να πιάσει αυτούς που προσπαθούν να αποκτήσουν πρόσβαση σε διακομιστές μέσω της υπηρεσίας SSH.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1

Στο κεφάλαιο αυτό θα δούμε ορισμούς, βασικές πληροφορίες καθώς και την αρχιτεκτονική των δικτύων των ηλεκτρονικών υπολογιστών. Επίσης θα αναφερθούμε και στις επιθέσεις που δέχονται τα δίκτυα και στο πως μπορούμε να τα προστατέψουμε.

1.1 ΕΙΣΑΓΩΓΗ

Εικόνα 1.1 : Διαδίκτυο
Πηγή: https://www.techfrog.gr/other-news/diodia-sto-internet-apo-tis-etaireies/

1.2 Ορισμός δικτύων υπολογιστών

Ως δίκτυο ορίζεται ένα σύνολο από δύο ή περισσότερους υπολογιστές που είναι συνδεδεμένοι μεταξύ τους με ένα ή περισσότερα φυσικά μέσα.

Τα δίκτυα δημιουργήθηκαν για να μπορέσουν να καλύψουν τις ανάγκες που προέκυψαν από την ραγδαία εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών. Κύριος σκοπός τους ήταν ο διαμοιρασμός των πόρων του συστήματος και η ανταλλαγή κάθε μορφής πληροφορία. Πόρος συστήματος λογίζεται τόσο το υλικό (hardware), π.χ. υπολογιστές, εκτυπωτές, scanners, σκληροί δίσκοι όσο και το λογισμικό (software), π.χ. προγράμματα, δεδομένα, υπηρεσίες. Έτσι οι πόροι είναι διαθέσιμοι σε όλους όσους είναι συνδεδεμένοι στο δίκτυο ανεξάρτητα από την φυσική τους θέση. Με αποτέλεσμα να εξοικονομούμε χρήματα, να αυξάνουμε την απόδοση των συστημάτων και να αποκτούμε κεντρικό έλεγχο.

1.3 Αρχιτεκτονική και είδη υπολογιστών

Η αρχιτεκτονική των δικτύων είναι αυτή που καθορίζει τον τρόπο διασύνδεσης των ηλεκτρονικών υπολογιστών και των λοιπών συσκευών έτσι ώστε να επιτρέπεται

στους χρήστες να διαμοιράζουν τόσο πληροφορίες όσο και συσκευές του δικτύου. Ένα δίκτυο δεδομένων αποτελείται από:

- Τερματικούς Κόμβους
- Υποδίκτυα
- Συσκευές Διασύνδεσης

Οι Τερματικοί Κόμβοι είναι υπεύθυνοι για τους πόρους του δικτύου. Τα υποδίκτυα είναι φυσικά μέσα μετάδοσης, πρωτόκολλα επικοινωνίας, τερματικοί κόμβοι και γενικά πόροι που μπορεί να είναι διαφορετικοί σε κάθε υποδίκτυο. Οι συσκευές διασύνδεσης είναι αυτές οι οποίες εξασφαλίζουν την επικοινωνία των τερματικών κόμβων σε ετερογενή υποδίκτυα.

Τα δίκτυα διαχωρίζονται ανάλογα με:

- Την γεωγραφική τους ανάπτυξη η οποία χωρίζεται σε:
  - ✓ **Δίκτυα ευρείας περιοχής (WAN,Wide Area Networks)** που μπορούν να καλύψουν αποστάσεις λίγων χιλιομέτρων μέσα σε μία πόλη ή και χιλιάδων χιλιομέτρων και να ενώσουν πόλεις, κράτη και ηπείρους. Π.χ. τέτοια δίκτυα είναι αεροπορικών εταιριών, τραπεζών, δημοσίου κλπ.
  - ✓ **Δίκτυα τοπικά ή μικρών αποστάσεων (LAN, Local Area Networks)** τα οποία είναι της τάξεως των μερικών εκατοντάδων μέτρων ή και μερικών χιλιομέτρων ώστε να καλύψουν μία επιχείρηση. Διαφέρουν από τα ευρείας ως προς τις τεχνικές λειτουργίας τους, και τα διακρίνει το μικρό κόστος ανά χρήστη, η μεγάλη ταχύτητα μεταφοράς, η επεκτασιμότητα, και η βελτιστοποίηση της χρήσης των μηχανημάτων.
  - ✓ **Αστικά Δίκτυα (MAN, Metropolitan Area Networks)** που όπως καταλαβαίνουμε και από το όνομα τους δεν επεκτείνονται περισσότερο από τα σύνορα μιας πόλης. Μπορούν να μεταδώσουν εικόνα, φωνή και δεδομένα ταχύτερα και ποιοτικότερα από τα τοπικά δίκτυα.
- Τον τηλεπικοινωνιακό φορέα εξυπηρέτησης ο οποίος χωρίζεται σε:
  - ✓ **Ιδιωτικά δίκτυα (Private Networks)**
  - ✓ **Δημόσια δίκτυα (Public Networks)**
- Την τεχνική προώθησης της πληροφορίας η οποία χωρίζεται σε:
  - ✓ **Δίκτυα μεταγωγής**
  - ✓ **Δίκτυα Ακρόασης**

- Το λειτουργικό σύστημα των ηλεκτρονικών υπολογιστών το οποίο χωρίζεται σε:

  - ✓ **Δίκτυο Windows**
  - ✓ **Δίκτυο Dos**
  - ✓ **Δίκτυο apletalk (Macintosh)**

- Το πρωτόκολλο επικοινωνίας το οποίο χωρίζεται σε:

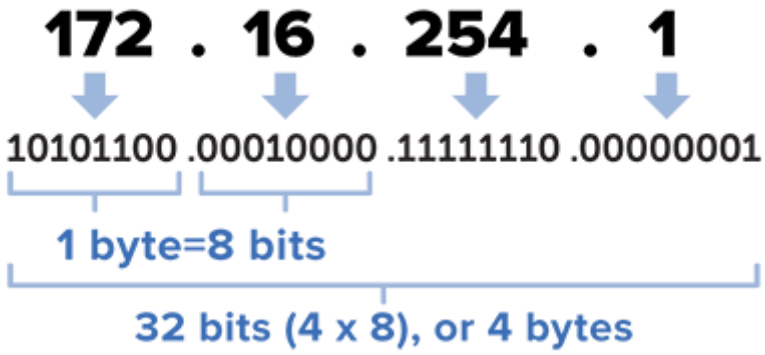
  - ✓ **Δίκτυα TCP/IP**
  - ✓ **Δίκτυα NET/BEUI**

- Την σχεδίαση η οποία χωρίζεται σε:

  - ✓ **Πελάτης – Διακομιστής (Client – Server)**
  - ✓ **Ομότιμα δίκτυα (Peer to Peer).**

1.4 IP διεύθυνση και μάσκα υποδικτύου

Η διεύθυνση IP είναι μια λογική αριθμητική διεύθυνση που αντιστοιχεί σε κάθε υπολογιστή, εκτυπωτή, διακόπτη Gigabit Ethernet , δρομολογητή ή οποιαδήποτε άλλη συσκευή σε δίκτυο βασισμένο σε TCP / IP, με καθένα από αυτά να διαθέτει μια μοναδική διεύθυνση IP. Οι διευθύνσεις IP είτε είναι διαμορφωμένες με μη αυτόματο τρόπο (στατική διεύθυνση IP) είτε έχουν διαμορφωθεί από διακομιστή DHCP. Μία διεύθυνση IP αποτελείται από 4 bytes δεδομένων. Ένα byte αποτελείται από 8 bits (ένα bit είναι ένα μόνο ψηφίο και θα μπορούσε να είναι μόνο 1 ή 0), επομένως έχουμε συνολικά 32 bits για κάθε διεύθυνση IP. Αυτό είναι ένα παράδειγμα διεύθυνσης IP στη δυαδική μορφή: 10101100. 00010000. 11111110.00000001. Για να απλοποιήσουμε τα πράγματα, η δεκαδική αναπαράσταση χρησιμοποιείται συνήθως για να γίνει αυτή η διεύθυνση IP: 172. 16. 254. 1. [1]



Εικόνα 1.2 : Ανάλυση IP διεύθυνσης
Πηγή: https://www.lifewire.com/what-is-ipv4-ipv6-2483315

Μια μάσκα υποδικτύου είναι ένας αριθμός 32 ή 128 bit που χωρίζει μια υπάρχουσα διεύθυνση IP σε ένα δίκτυο TCP / IP. Χρησιμοποιείται από το πρωτόκολλο TCP / IP για να προσδιορίσει εάν ένας κεντρικός υπολογιστής βρίσκεται στο τοπικό υποδίκτυο ή σε απομακρυσμένο δίκτυο. Η μάσκα υποδικτύου χωρίζει τη διεύθυνση IP σε διεύθυνση δικτύου και διεύθυνση κεντρικού υπολογιστή, οπότε προσδιορίζεται ποιο τμήμα της διεύθυνσης IP προορίζεται για το δίκτυο και ποιο τμήμα είναι διαθέσιμο για χρήση από τον κεντρικό υπολογιστή. Αφού δοθεί η διεύθυνση IP και η μάσκα υποδικτύου της, μπορεί να καθοριστεί η διεύθυνση δικτύου (υποδίκτυο) ενός κεντρικού υπολογιστή. Συνήθως, οι υπολογιστές υποδικτύου είναι άμεσα διαθέσιμοι σε απευθείας σύνδεση που βοηθούν να διαιρέσετε ένα δίκτυο IP σε υποδίκτυα. [2]

1.5 TCP/IP

Αποτελώντας την ραχοκοκαλιά του παγκόσμιου ιστού αλλά και των περισσότερων επιμέρους δικτύων, το TCP/IP αποτελεί μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Η ονομασία TCP/IP προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων της συλλογής: το Transmission Control Protocol (Πρωτόκολλο Ελέγχου Μετάδοσης) και το Internet Protocol (Πρωτόκολλο Διαδικτύου).

Αναλυτικότερα, η συλλογή αυτή είναι οργανωμένη σε επίπεδα (layers) καθένα από τα οποία καλείται να διαχειριστεί συγκεκριμένα προβλήματα μεταφοράς δεδομένων και να παρέχει μια καθορισμένη υπηρεσία στα υψηλότερα επίπεδα. Τα ανώτερα επίπεδα είναι πιο κοντά στη λογική του χρήστη και εξετάζουν πιο αφηρημένα δεδομένα. Στηρίζονται στα πρωτόκολλα των χαμηλότερων επιπέδων για την μετάφραση δεδομένων σε μορφές οι οποίες είναι δυνατόν να διαβιβαστούν με φυσικά μέσα. [3]

1.6 Πρωτόκολλο

Τι είναι όμως το πρωτόκολλο, ως δομική μονάδα της συλλογής TCP/IP; Στην ουσία αποτελεί ένα σύνολο κανόνων συμφωνημένων και από τα δυο επικοινωνούντα μέρη με σκοπό την εξυπηρέτηση της μεταξύ τους ανταλλαγής πληροφοριών. Το πρωτόκολλο επικοινωνίας είναι δηλαδή μια δέσμη κανόνων στους οποίους στηρίζεται η επικοινωνία των συσκευών (συνήθως, αλλά όχι πάντα, υπολογιστών) σε ένα δίκτυο.

Οι κανόνες αυτοί καθορίζουν τη μορφή, το χρόνο και τη σειρά μετάδοσης των πληροφοριών στο δίκτυο. Εκτελούν, επίσης, έλεγχο και διόρθωση σφαλμάτων στη διάρκεια μετάδοσης των πληροφοριών.

Υπάρχουν διάφορα πρωτόκολλα επικοινωνίας, τα οποία προκαλούν πολλές φορές σύγχυση στους χρήστες. Ευτυχώς σήμερα, παρόλο που δεν υπάρχει κάποιο που να είναι καθιερωμένο πρότυπο, με την εξάπλωση των Windows και του Διαδικτύου, τα πρωτόκολλα που είναι περισσότερο διαδεδομένα είναι το TCP/IP, το NETBEUI και το IPX/SPX [4]

ΚΕΦΑΛΑΙΟ 2

Στο κεφάλαιο αυτό θα δούμε βασικές έννοιες ασφαλείας συστημάτων καθώς και απειλές.

2.1 Ορισμός

Η Ασφάλεια Πληροφοριακών Συστημάτων έχει ως στόχο την προστασία πολύτιμων πόρων ενός οργανισμού, είτε αυτές είναι πληροφορίες, είτε λογισμικό ή υλικό. Το στόχο αυτό τον εκπληρώνει μέσα από την επιλογή και εφαρμογή κατάλληλων μηχανισμών έτσι ώστε να προστατεύονται οι φυσικοί και οικονομικοί πόροι, η φήμη, η νόμιμη θέση, οι εργαζόμενοι και γενικά όλα τα υλικά και άυλα περιουσιακά στοιχεία ενός οργανισμού.

Σε κάθε οργανισμό – επιχείρηση πρέπει να εφαρμόζονται κατάλληλη κανόνες ασφαλείας έτσι ώστε να αποφεύγεται η παρεμπόδιση της λειτουργίας της. Διότι παρατηρείται συχνά στα πλαίσια της Ασφάλειας Πληροφοριακών Συστημάτων να επιβάλλονται αυστηροί, ενοχλητικοί κανόνες και διαδικασίες σε χρήστες, διαχειριστές και συστήματα με αποτέλεσμα να δυσκολεύουν την λειτουργία της. Τέλος οι κανόνες ασφαλείας πρέπει να τίθενται με τέτοιο τρόπο ώστε να συμβάλουν στην εύρυθμη λειτουργία και στην κερδοφορία του οργανισμού – επιχείρησης. [5]

2.2 Βασικές έννοιες

Στα πλαίσια της Ασφάλειας Πληροφοριακών Συστημάτων όλοι οι έλεγχοι καθώς και όλες οι απειλές και τα τρωτά σημεία βασίζονται στις τρείς θεμελιώδες αρχές. Αυτές οι αρχές είναι οι εξής:

- **Εμπιστευτικότητα (Confidentiality)**: αφορά την αποφυγή αποκάλυψης του περιεχομένου ενός μηνύματος σε μη εξουσιοδοτημένα άτομα. Απώλεια εμπιστευτικότητας μπορεί να συμβεί με πολλούς τρόπους, π.χ η εσφαλμένη ανάθεση δικαιωμάτων πρόσβασης σε χρήστη σε ένα δίκτυο, ή η εσκεμμένη διαρροή πληροφοριών μιας εταιρίας.

  Η εμπιστευτικότητα στα δίκτυα εξασφαλίζεται με χρήση πρωτοκόλλων ασφαλείας, με υπηρεσίες ελέγχου και πιστοποίησης ταυτότητας καθώς και με υπηρεσίες κρυπτογράφησης δεδομένων.

- **Ακεραιότητα (Integrity)**: είναι η επιβεβαίωση ότι τα δεδομένα που έχουν αποσταλεί-παραληφθεί είναι πλήρη χωρίς καμία αλλοίωση. Στον κόσμο της πληροφορικής ακεραιότητα είναι η πρόληψη μη εξουσιοδοτημένης μεταβολής (εγγραφή, διαγραφή, δημιουργία) πληροφοριών.

Η ακεραιότητα στα δίκτυα εξασφαλίζεται με χρήση τειχών ασφαλείας (firewall), πολιτικών ασφαλείας επικοινωνιών καθώς και με υπηρεσίες ανίχνευσης παρείσφρησης.

- **Διαθεσιμότητα (Availability)**: είναι αυτή που εξασφαλίζει την έγκυρη και αξιόπιστη πρόσβαση σε υπολογιστικούς πόρους και δεδομένα από εγκεκριμένους χρήστες. Με τον όρο διαθεσιμότητα εννοούμε ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργούν, άσχετα με το αν υπάρχουν κάποιες διαταραχές στο δίκτυο (π.χ διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα η επιθέσεις).

  Η Διαθεσιμότητα στα δίκτυα εξασφαλίζεται με περιορισμένη ανοχή σφαλμάτων, με χρήση αντιγράφων ασφαλείας, με έλεγχο πρόσβασης χρηστών στο σύστημα και με χρήση αξιόπιστων διαδικασιών και μηχανισμών ασφαλείας δικτύων. [6]

2.3 Κοινές απειλές

Τα Υπολογιστικά Συστήματα είναι ευάλωτα σε διάφορους τύπους απειλών που μπορούν να προκαλέσουν διάφορες βλάβες με αποτέλεσμα σημαντικών απωλειών. Οι βλάβες ποικίλουν, από λάθη που επηρεάζουν την βάση δεδομένων μέχρι και φυσικές καταστροφές που μπορούν να διαλύσουν ολόκληρα υπολογιστικά κέντρα. Απώλειες επίσης μπορούν να προκύψουν από hackers, από δήθεν έμπιστους χρήστες που εξαπατούν ένα σύστημα ακόμα και από απρόσεκτους χρήστες που εισάγουν λανθασμένα δεδομένα στο σύστημα. Πολλές απώλειες είναι πιθανών να μην γίνουν ποτέ αντιληπτές όπως και πολλές άλλες να μην αποκαλυφτούν πότε για λόγους αρνητικής δημοσιότητας. Ο στόχος των απειλών είναι να βλάψουν τις τρείς θεμελιώδες αρχές που αναφέρθηκαν παραπάνω (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) .

Οι πιο κοινές απειλές κατά τις Ασφάλειας Πληροφοριακών Συστημάτων είναι οι εξής:

- **Σφάλματα και παραλείψεις**: Τα σφάλματα και οι παραλείψεις που δημιουργούνται από απλούς χρήστες, διαχειριστές συστημάτων καθώς και προγραμματιστές επηρεάζουν άμεσα ή έμμεσα την ασφάλεια δεδομένων. Κάποια σφάλματα εγκατάστασης και συντήρησης συστημάτων όπως και κάποια προγραμματιστικά λάθη (bugs) μπορεί να περάσουν αδιάφορα αλλά μπορεί να είναι και καταστροφικά για το σύστημα.
- **Εξαπάτηση**: Η αξιοποίηση των υπολογιστικών συστημάτων δεν γίνεται πάντα για καλό σκοπό, πολλές φορές είναι κακόβουλη και έχει ως στόχο την εξαπάτηση των χρηστών. Συνήθως χτυπάνε πιο πολύ τα χρηματοπιστωτικά συστήματα, τα συστήματα απογραφής, τα σχολικά συστήματα και τα

τηλεφωνικά συστήματα. Η εξαπάτηση χρηστών μπορεί να γίνει από γνώστες του συστήματος δηλαδή από κάποιους που εργάζονται στην επιχείρηση αλλά μπορεί να γίνει και από εξωτερικούς χρήστες.

- **Δολιοφθορά Σαμποτάζ**: Η δολιοφθορά- σαμποτάζ συνήθως πραγματοποιείτε από εργαζόμενους της εταιρίας που νιώθουν ότι η δουλειά τους δεν ανταμείβεται σωστά ή βαριούνται ή παρενοχλούνται στο χώρο εργασίας τους. Αυτό το πετυχαίνουν είτε καταστρέφοντας υλικό είτε αλλοιώνοντας δεδομένα με διάφορους τρόπους είτε εισάγοντας ιογενείς υλικό στον κώδικα.
- **Απώλεια φυσικών υποδομών**: Εδώ εντάσσονται οι απώλειες που μπορεί να έχουμε λόγο φυσικών καταστροφών, διακοπής ρεύματος και επικοινωνιών, προβλήματα ύδρευσης, προβλήματα μεταφοράς και μετακινήσεις.
- **Λογισμικό κακόβουλου τύπου**: Εδώ εντάσσονται τα λογισμικά που έχουν ως σκοπό να βλάψουν το σύστημα. Θα μιλήσουμε αναλυτικά για αυτά στο επόμενο κεφάλαιο.
- **Βιομηχανική κατασκοπεία**: Είναι η υποκλοπή απόρρητων πληροφοριών μίας επιχείρησης από μία άλλη με σκοπό την βελτίωση της έναντι της άλλης. Επίσης υποκλοπή γίνεται και κατά τις κυβέρνησης με σκοπό την βελτίωση των δεικτών ανταγωνιστικότητας εγχώριων επιχειρήσεων. Η απειλή αυτή είναι δύσκολο να καταπολεμηθεί γιατί ναι μεν με την ασφάλεια πληροφοριακών συστημάτων η υποκλοπή πληροφοριών γίνεται σχεδόν αδύνατη από την άλλη όμως δεν μπορεί να καταπολεμηθεί η πώληση ιδιωτικών πληροφοριών από εξουσιοδοτημένους υπαλλήλους.

2.4 Δικτυακές επιθέσεις

Στις μέρες μας οι επιθέσεις δικτύων έχουν πάρει μεγάλες διαστάσεις και προκαλούν τεράστια προβλήματα σε εταιρίες, οργανισμούς αλλά και χρήστες. Κάποιες επιθέσεις είναι ενεργητικές και κάποιες παθητικές. Οι ενεργητικές έχουν σκοπό την τροποποίηση ή και καταστροφή των δικτυακών δεδομένων ενώ οι παθητικές την υποκλοπή τους. Παρακάτω παρατίθενται οι συνήθης δικτυακές επιθέσεις.

2.4.1 Απόκτηση πληροφοριών για το σύστημα

Η επίθεση αυτή έχει ως σκοπό την εξέταση της αρχιτεκτονικής και του συστήματος ενός δικτύου, την εύρεση των υπηρεσιών που λειτουργούν και το μέρος που αυτές εκτελούνται όπως και το είδος του λογισμικού που χρησιμοποιείται (mail servers, DNS servers, λειτουργικό). Η επίθεση μπορεί να γίνει με την παρουσία του κακόβουλου σε ένα σημείο από όπου θα μπορεί να παρακολουθεί την κίνηση από και προς το δίκτυο (παθητική επίθεση). Επίσης μπορεί να γίνει και με κάποια εργαλεία δικτύου όπως είναι το tracerout, ping, DNS zone transfers, IPscanners, Nmap και άλλα (ενεργητική επίθεση).

2.4.2 Μη εξουσιοδοτημένη πρόσβαση

Σκοπός της μη εξουσιοδοτημένης πρόσβασης είναι η υποκλοπή κωδικών πρόσβασης. Αυτό επιτυγχάνεται μέσω Social Engineering (αφέλεια διαχειριστών) που είναι ο πιο εύκολος τρόπος υποκλοπής, μέσω χρήσης αδύναμων κωδικών (ημερομηνίες γέννησης, λέξεις με νόημα) ή κακής προστασίας των κωδικών (αποστολή κωδικού χωρίς κρυπτογράφηση). Τέλος λόγο της μεγάλης ανάπτυξης των ασύρματων δικτύων η μη εξουσιοδοτημένη πρόσβαση είναι πολύ πιο εύκολη διότι η ασύρματη μετάδοση παρουσιάζει μεγάλα κενά ασφαλείας σε συνδυασμό με τη χρήση αδύναμων πρωτοκόλλων(π.χ WEP Wired Equivalent Privacy).

2.4.3 Υποκλοπή και παραποίηση

Ο τύπος αυτός επίθεσης έχει ως σκοπό την μη εξουσιοδοτημένη παρακολούθηση δικτυακής κίνησης. Οι επιθέσεις αυτές γίνονται πιο πολύ σε δίκτυα δορυφόρων, κινητών, ασύρματα και γενικός σε όλα τα ευπαθή. Για αυτό πρέπει τα δεδομένα να κρυπτογραφούνται όταν διασχίζουν ένα δίκτυο ώστε να μην είναι ευάλωτα στην υποκλοπή.

Οι επιθέσεις υποκλοπής και παραποίησης χωρίζονται σε δύο κατηγορίες τις ενεργητικές και τις παθητικές. Παθητικές ονομάζονται οι επιθέσεις που παρακολουθούν και καταγράφουν μεταδόσεις χωρίς αδεία από τον παραλήπτη ή τον αποστολέα. Ενεργητικές ονομάζονται οι επιθέσεις που γίνονται όταν κάποιος παρεμβληθεί σε μία επικοινωνία και προσπαθήσει είτε να υποκλέψει στοιχεία είτε να υποκριθεί ότι είναι κάποιος τρίτος φορέας. Τέτοιες επιθέσεις είναι το ARP poisoning, το TCP session hijacking και το DNS cache poisoning.

- **ARP poisoning**: Είναι τύπος παραβίασης δικτύου και βασίζεται στο πρωτόκολλο ARP. Ο κακόβουλος χρήστης προσπαθεί να μπερδέψει άλλους host ώστε να στείλουν τα πλαίσια δεδομένων τους σε άλλον υπολογιστή χωρίς να το αντιληφθούν μεταδίδοντας λανθασμένα πακέτα ARP. Επίσης μπορεί και να αποκλείσει έναν host από ένα δίκτυο. [7]
- **TCP session hijacking**: Είναι η διαδικασία κατάληψης μιας ενεργής σύνδεσης. Αυτή η επίθεση έχει ως σκοπό την παράκαμψη της διαδικασίας ελέγχου ταυτότητας και απόκτηση πρόσβασης σε έναν υπολογιστή. Έτσι επιτυγχάνεται εύκολη πρόσβαση σε πόρους και ευαίσθητες πληροφορίες, όπως κωδικοί τραπεζών, mail και πολλά άλλα. [8]
- **DNS cache poisoning**: Είναι η επίθεση που έχει ως σκοπό την εισαγωγή ψεύτικων πληροφοριών DNS στον εξυπηρετητή. [9]

2.5 Κακόβουλο λογισμικό (MALWARE)

Ο όρος malware είναι μία σύντμηση των λέξεων malicious software, και αναφέρεται σε κάθε είδος λογισμικό που έχει ως σκοπό να βλάψει κάποιον υπολογιστή ή διακομιστή ή δίκτυο και γενικά οτιδήποτε υπολογιστικό σύστημα. Παρακάτω παρουσιάζονται τα κύρια είδη κακόβουλου λογισμικού. [10]

2.5.1 Σκουλήκια (WORMS)

Σκουλήκι ονομάζεται ένα πρόγραμμα το οποίο διαδίδεται αντιγράφοντας τον εαυτό του από υπολογιστή σε υπολογιστή μέσα από τοπικά δίκτυα ή και μέσω διαδικτύου. Αυτό το επιτυγχάνει μέσω του ηλεκτρονικού ταχυδρομείου ή μέσω της απομακρυσμένης σύνδεσης. Η λειτουργία του έχει πολλές πλευρές, μπορεί να συμπεριφερθεί είτε ως ιός είτε να εισάγει δούρειους ίππους είτε να εκτελέσει οποιαδήποτε καταστροφική ενέργεια. Τα σκουλήκια έχουν τρία στάδια λειτουργίας.

1. **Μόλυνση**, σε αυτή τη φάση το σκουλήκι είναι ανενεργό και περιμένει να ενεργοποιηθεί μετά από κάποιο ερέθισμα. Το ερέθισμα αυτό μπορεί να είναι η εκτέλεση μίας συγκεκριμένης εντολής ή η έλευση μίας συγκεκριμένης ημερομηνίας ή η υπέρβαση κάποιου αποθηκευτικού ορίου στο δίσκο ή η παρουσία κάποιου άλλου προγράμματος.
2. **Επίθεση**, σε αυτή τη φάση το σκουλήκι ενεργοποιείται και εκτελεί τη λειτουργία για την οποία έχει σχεδιαστεί.
3. **Εξάπλωση**, σε αυτή τη φάση το σκουλήκι προσπαθεί να βρει νέα συστήματα προς μόλυνση και αυτό το επιτυγχάνει με εξέταση των πινάκων που περιέχουν διευθύνσεις απομακρυσμένων συστημάτων.

2.5.2 Ιοί (VIRUSES)

Με τον όρο ιό ορίζουμε ένα πρόγραμμα το οποίο μπορεί να μολύνει άλλα προγράμματα τροποποιώντας τα με σκοπό να βλάψει σημαντικά αρχεία. Σε αντίθεση με τα σκουλήκια οι ιοί δεν εμπεριέχουν μηχανισμούς αυτόματης εξάπλωσης σε άλλους υπολογιστές. Για αυτό το λόγο οι ιοί εξαπλώνονται συνήθως μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου που εμπεριέχουν τον ιό ως επισυναπτόμενο αρχείο.

2.5.3 Δούρειοι ίπποι (TROJAN HORSES)

Η ονομασία Δούρειος ίππος προήλθε από τον γνωστό Δούρειο ίππο του τρωικού πολέμου. Όπως τότε ο Δούρειος ίππος προσφέρθηκε ως δώρο από τον Οδυσσέα προς τους Τρώες με σκοπό να τους ξεγελάσει και να καταφέρουν οι κρυμμένοι στρατιώτες μέσα στον Δούρειο ίππο να εισέλθουν στην Τροία. Έτσι και σήμερα οι Δούρειοι ίπποι στους υπολογιστές ενώ φαίνονται και συμπεριφέρονται σαν κανονικά και χρήσιμα προγράμματα περιέχουν βλαβερό κώδικα που

ενεργοποιείται όταν εκτελεστεί το πρόγραμμα. Μία συνήθης ενέργεια είναι η καταγραφή και αποστολή ευαίσθητων προσωπικών δεδομένων όπως είναι username και password ή αριθμοί πιστωτικών καρτών στον δημιουργό τους. Τέλος οι Δούρειοι ίπποι είναι σαν τους ιούς δεν εξαπλώνονται μόνοι τους.

2.5.4 BOTS

Το "Bot" προέρχεται από τη λέξη "ρομπότ" και είναι μια αυτοματοποιημένη διαδικασία που αλληλεπιδρά με άλλες υπηρεσίες δικτύου. Τα bots ως προγράμματα ξεκίνησαν για την συλλογή πληροφοριών, όπως ανιχνευτές ιστού , ή η αυτόματη αλληλεπίδραση με τα Instant Messaging (IM) , το Internet Relay Chat (IRC) ή άλλες διεπαφές ιστού. Ένα κακόβουλο bot είναι από μόνο του ένα κακόβουλο λογισμικό που έχει σχεδιαστεί για να μολύνει έναν κεντρικό υπολογιστή και να συνδεθεί πίσω από έναν κεντρικό διακομιστή ή διακομιστές που λειτουργούν ως κέντρο ελέγχου για ένα ολόκληρο δίκτυο συμβαλλόμενων συσκευών ή "botnet". Με ένα botnet, οι επιτιθέμενοι μπορούν να εκτοξεύσουν επιθέσεις πλημμυρών τύπου "απομακρυσμένου ελέγχου" κατά του στόχου (στόχων) τους. Τα botnets χρησιμοποιούνται για διάφορους κακόβουλους σκοπούς όπως η φιλοξενία ιστοσελίδων εξαπάτησης (phishing), αποστολή μηνυμάτων spam, διενέργεια κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS), κ.α. Το κίνητρο πίσω από τη δημιουργία τους είναι στην συντριπτική πλειοψηφία οικονομικό.

2.5.5 Rootkits

Ένα rootkit είναι λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές με το να ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών. Ο όρος rootkit είναι μια συνένωση των λέξεων "root" (το παραδοσιακό όνομα του προνομιούχου λογαριασμού σε λειτουργικά συστήματα τύπου Unix) και της λέξης "kit". Τυπικά, ένας εισβολέας εγκαθιστά ένα rootkit σε έναν υπολογιστή μόλις αποκτήσει πρόσβαση σε επίπεδο υπερχρήστη είτε με την αξιοποίηση γνωστών κενών στην ασφάλεια στου λειτουργικού είτε με την απόκτηση ενός κωδικού πρόσβασης (είτε με απευθείας επίθεση στην κρυπτογράφηση, είτε μέσω της κοινωνικής μηχανικής). Το πρόβλημα που εμφανίζεται είναι ότι τα λογισμικά αντιμετώπισης κατά βάση πραγματοποιούν μια ανίχνευση σε ένα τροποποιημένο σύστημα και τα rootkits έχουν την δυνατότητα να διαστρεβλώσουν ακόμα και τα ίδια τα προγράμματα εξυγίανσης του ηλεκτρονικού υπολογιστή.

Αν και τα rootkits από μόνα τους δεν αποτελούν κάποια απειλή , υφίστανται μερικοί κίνδυνοι που προκύπτουν από την χρήση τους όπως είναι η αδυναμία εξυγίανσης ενός συστήματος και κατά αποτέλεσμα η απώλεια του εξ ολοκλήρου

ελέγχου του από τον ιδιοκτήτη ή η υποκλοπή σημαντικών πληροφοριών (π.χ. αριθμός πιστωτικής κάρτας, κωδικοί πρόσβασης, κ.α.)

Η αντιμετώπιση των rootkits εξαρτάται από την γενιά τους. Παρόλα αυτά υπάρχουν κάποιες μέθοδοι αποκάλυψης και πρόληψης από αυτά. Τα memory dumps ,η μέθοδος βασισμένη στην συμπεριφορά, η signature based method , η difference based method και το εναλλακτικό αξιόπιστο μέσο αποθήκευσης είναι μερικές από αυτές.

2.5.6 Κερκόπορτα (TRAPDOOR)

Ως κερκόπορτα ορίζεται μία μυστική πύλη σε ένα πρόγραμμα, εφαρμογή, λειτουργικό σύστημα ή διαδικτυακή υπηρεσία που δίνει πρόσβαση σε όποιον τη γνωρίζει στο σύστημα παρακάμπτοντας τις διαδικασίες ελέγχου πρόσβασης. Οι κερκόπορτες δημιουργούνται συνήθως από τους προγραμματιστές κατά την διάρκεια εκσφαλμάτωσης ή δοκιμής του συστήματος και εν συνεχεία κλείνονται. Μερικές φορές αφήνονται ανοιχτές από αμέλεια η επίτηδες και αποτελούν τρύπες ασφαλείας. Επιπρόσθετα είναι σχεδόν αδύνατον να κλείσουν μετά και έτσι απαιτείται διαμόρφωση (format) του σκληρού δίσκου.

Πιο συγκεκριμένα, κατά την διαδικασία αυθεντικοποίησης, ο προγραμματιστής προκειμένου να έχει ειδικά προνόμια και για να αποφύγει την διαδικασία εγκατάστασης και αυθεντικοποίησης, εισάγει στον κώδικά του κερκόπορτες. Κερκόπορτα μπορεί να είναι μια ειδική ακολουθία εισόδου ή κώδικας που ενεργοποιείται από συγκεκριμένο χρήστη ή ακόμα και μια συγκεκριμένη ακολουθία γεγονότων.

Η κερκόπορτα αποτελεί πάγια τακτική εισβολέων αφού έχουν αποκτήσει πρόσβαση σε ένα σύστημα να την δημιουργούν και να την αφήνουν ανοιχτή ώστε να μπορούν εύκολα και γρήγορα να επανασυνδεθούν στον μέλλον.

Η καλύτερη προστασία από κερκόπορτες είναι η πρόληψη κατά τις διαδικασίες ανάπτυξης και συντήρησης λογισμικού.

2.5.7 Λογικές βόμβες (LOGIC BOMBS)

Μια λογική βόμβα είναι ένα κομμάτι κώδικα που εισάγεται σκοπίμως σε ένα σύστημα λογισμικού που θα εκπέμπει μια κακόβουλη λειτουργία όταν πληρούνται συγκεκριμένες προϋποθέσεις. Για παράδειγμα, ένας προγραμματιστής μπορεί να κρύψει ένα κομμάτι κώδικα που ξεκινά τη διαγραφή αρχείων (όπως μια ενεργοποίηση βάσης δεδομένων μισθοδοσίας), σε περίπτωση που τερματιστεί από την εταιρεία, ή παρέρθει η έλευση μιας ημερομηνίας ή η μνήμη του σκληρού δίσκου του συστήματος να ξεπεράσει ένα συγκεκριμένο ποσοστό κ.α.

Μερικές φορές όμως οι λογικές βόμβες αναπτύσσονται από τους προγραμματιστές και για την πρόληψη και αποφυγή επιθέσεων στο σύστημα. Αυτές μπορούν να λειτουργήσουν ως honeytokens, δηλαδή να αποτελούν μια ψηφιακή

οντότητα που θα είναι ευάλωτη σε επιθέσεις και θα λειτουργεί σαν συναγερμός σε περίπτωση μη εξουσιοδοτημένης χρήσης.

ΚΕΦΑΛΑΙΟ 3

Η προστασία των δικτύων και γενικά των υπολογιστικών συστημάτων είναι από πλευρά τεχνικής αλλά οικονομικής φύσης ασύμφορο να επιτευχθεί για όλα τα είδη των επιθέσεων. Για να μπορέσει κάποιος να προσδιορίσει τις κατάλληλες ενέργειες για κάθε επίθεση και αυτό να το κάνει με επιτυχία πρέπει να εξετάσει αρκετές παραμέτρους, οι οποίες έχουν να κάνουν με συστήματα που θέλει να προστατέψει, με το είδος των υπηρεσιών που παρέχει το καθένα, με την δομή του δικτύου και τις απαιτήσεις των χρηστών του. Στο κεφάλαιο αυτό θα δούμε κάποια βασικά συστατικά μιας υλοποίησης ασφαλείας σε ένα δίκτυο.

3.1 Αντιβιοτικά (ANTIVIRUS)

Antivirus είναι ένα λογισμικό - ένα πρόγραμμα το οποίο μας βοηθάει να εντοπίσουμε ιούς, spywares, adwares, trojans και άλλα τέτοια κακόβουλα λογισμικά που μπορεί να έχει κολλήσει ο υπολογιστής μας.

Το antivirus είναι η άμυνα ενάντια σε τέτοια κακόβουλα λογισμικά που μπορεί να δημιουργούνε προβλήματα στον υπολογιστή μας, να μας υποκλέπτουν προσωπικά δεδομένα ή να μας εμφανίζουν ενοχλητικές διαφημίσεις.

Είναι ένα πρόγραμμα το οποίο εγκαθιστάμε στον υπολογιστή μας και μπορούμε άμεσα να "σκανάρουμε" όλους μας τους σκληρούς δίσκους για εντοπισμό και εξάλειψη τέτοιων κακόβουλων προγραμμάτων.

Ένα άλλο θετικό είναι ότι με τα antivirus υπάρχει real time προστασία, που σημαίνει πολύ απλά ότι οτιδήποτε κάνουμε αυτή τη στιγμή, σκανάρεται και αν εντοπίσει κάτι κακόβουλο, είτε μας προειδοποιεί, είτε το μπλοκάρει είτε το σβήνει αμέσως. Έτσι μας αποτρέπει να κολλήσουμε ιούς και άλλα τέτοια.

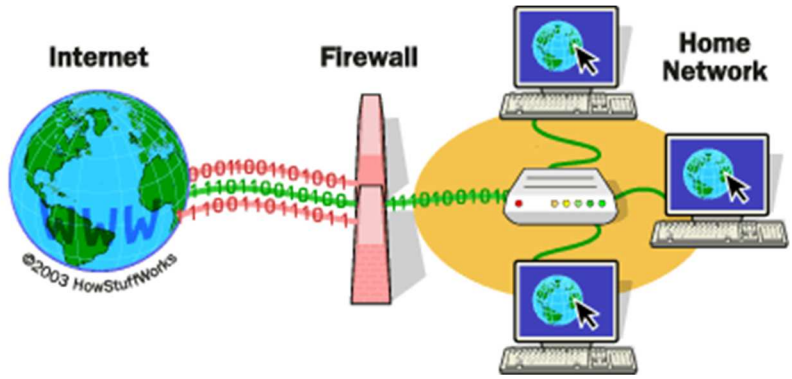
Καλό είναι να το κάνουμε τακτικά update ώστε να μένει ενημερωμένο για τα πιο καινούρια κακόβουλα προγράμματα και ιούς και να είναι σε θέση να τα εντοπίζει.

3.2 Τείχος προστασίας (FIREWALL)

Στην επιστήμη των υπολογιστών ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό

εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.



Εικόνα 3.1 : Πως δουλεύει το Firewall.
Πηγή: https://computer.howstuffworks.com/firewall.htm

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

3.2.1 Τύποι τειχών προστασίας

Ανάλογα με τον τρόπο λειτουργίας τους τα τείχη προστασίας μπορούν να κατηγοριοποιηθούν σε διαφορετικούς τύπους. Η πιο απλή μορφή ενός τείχους προστασίας δεν αποθηκεύει καθόλου πληροφορία για την κατάσταση των πελατών που εξυπηρετεί, λειτουργεί δηλαδή σε μία stateless κατάσταση και απλά φιλτράρει τη δικτυακή κίνηση με κριτήριο την προέλευση και τον προορισμό αυτής. Αυτού του τύπου τα τείχη προστασίας συχνά δεν αποθηκεύουν πληροφορίες για συνδέσεις που έχουν αφετηρία το εσωτερικό του δικτύου. Όταν πραγματοποιείται μία σύνδεση από το εσωτερικό δίκτυο προς το Διαδίκτυο το τείχος προστασίας επιτρέπει τη διέλευση δεδομένων από το εξωτερικό προς το εσωτερικό. Τέτοιου είδους τείχη προστασίας μπορούν όμως να παρακαμφθούν σχετικά εύκολα. Ο δεύτερος τύπος τειχών προστασίας κρατάει πληροφορίες για την κατάσταση των πελατών που εξυπηρετεί και τις αποθηκεύει σε έναν πίνακα, οπότε και βρίσκεται σε μία stateful κατάσταση.

3.2.2 Αδυναμίες και προβλήματα τειχών προστασίας

Τα τείχη προστασίας είναι ευρέος διαδεδομένα λόγω της εύκολης τοποθέτησής τους στα δίκτυα. Η ασφάλεια στα δίκτυα που μας προσφέρουν είναι σαφώς μεγάλη αλλά θα πρέπει να ξέρουμε ότι τα τείχη προστασίας παρουσιάζουν και κάποιες ευπάθειες. Δηλαδή έχουν και αυτά κάποιες αδυναμίες και προβλήματα τα οποία έχουν εντοπιστεί και προσπαθούν να αντιμετωπιστούν. Αναφορικά τα προβλήματα αυτά είναι:

- Το τείχος προστασίας δεν μπορεί να προστατέψει το δίκτυο από επιθέσεις που καταφέρνουν και το παρακάμπτουν.
- Το τείχος προστασίας δεν μπορεί να προστατέψει το δίκτυο από απειλές και επιθέσεις που βρίσκονται είδη εντός του δικτύου.
- Το τείχος προστασίας δεν μπορεί να προστατέψει τους υπολογιστές του δικτύου από την μεταφορά και διάδοση κακόβουλου λογισμικού που είναι ενσωματωμένο σε αρχεία και εφαρμογές.
- Το τείχος προστασίας σε ορισμένες περιπτώσεις που υπάρχει μεγάλου όγκου δικτυακή ροή καθίσταται αδύνατο να την παρακολουθήσει και έτσι επιτρέπει τη μεταφορά κακόβουλων πακέτων δεδομένων στο δίκτυο.

3.3 IDS – Συστήματα ανίχνευσης επιθέσεων

Ένα σύστημα ανίχνευσης εισβολών (IDS) είναι μια συσκευή ή εφαρμογή λογισμικού που παρακολουθεί ένα δίκτυο ή συστήματα για κακόβουλη δραστηριότητα ή παραβιάσεις πολιτικής. Κάθε κακόβουλη δραστηριότητα ή παραβίαση αναφέρεται συνήθως είτε σε διαχειριστή είτε συλλέγεται κεντρικά χρησιμοποιώντας ένα σύστημα πληροφοριών ασφαλείας και διαχείρισης συμβάντων (SIEM). Ένα σύστημα SIEM συνδυάζει έξοδο από πολλαπλές πηγές και χρησιμοποιεί τεχνικές φιλτραρίσματος συναγερμών για να διακρίνει την κακόβουλη δραστηριότητα από ψευδείς συναγερμούς. [παραπομπή που απαιτείται]

Οι τύποι IDS κυμαίνονται από ένα μόνο υπολογιστή σε ένα μεγάλο δίκτυο. Οι πιο συνηθισμένες ταξινομήσεις είναι τα συστήματα ανίχνευσης εισβολής με βάση το δίκτυο (NIDS) και τα συστήματα ανίχνευσης εισβολής με βάση τον κεντρικό υπολογιστή host (HIDS) . Ένα σύστημα που παρακολουθεί σημαντικά αρχεία λειτουργικού συστήματος είναι ένα παράδειγμα ενός HIDS, ενώ ένα σύστημα που αναλύει την εισερχόμενη κίνηση δικτύου είναι ένα παράδειγμα ενός NIDS. Είναι επίσης δυνατή η ταξινόμηση του IDS με προσέγγιση ανίχνευσης: οι πιο γνωστές παραλλαγές είναι η ανίχνευση που βασίζεται σε υπογραφή (αναγνωρίζοντας κακά πρότυπα, όπως κακόβουλα προγράμματα). και ανίχνευση με βάση την ανωμαλία (ανίχνευση αποκλίσεων από ένα μοντέλο "καλής" κυκλοφορίας, το οποίο συχνά βασίζεται στη μηχανική μάθηση). Ορισμένα προϊόντα IDS έχουν τη δυνατότητα να ανταποκρίνονται στις εντοπισμένες εισβολές. Τα συστήματα με δυνατότητες απόκρισης αναφέρονται συνήθως ως σύστημα πρόληψης εισβολής .

3.3.1 NETWORK – BASED IDS (Συστήματα ανίχνευσης εισβολής με βάση το δίκτυο)

Τα συστήματα ανίχνευσης εισβολής με βάση το δίκτυο λειτουργούν διαφορετικά από τα IDS που βασίζονται σε κεντρικούς υπολογιστές. Η φιλοσοφία σχεδιασμού ενός IDS βασισμένου σε δίκτυο είναι η σάρωση πακέτων δικτύου στο δρομολογητή ή στο επίπεδο κεντρικού υπολογιστή, ο έλεγχος των πληροφοριών πακέτων και η καταγραφή οποιωνδήποτε ύποπτων πακέτων σε ένα ειδικό αρχείο καταγραφής με εκτεταμένες πληροφορίες. Με βάση αυτά τα ύποπτα πακέτα, ένα IDS με βάση το δίκτυο μπορεί να σαρώσει τη δική του βάση δεδομένων με γνωστές υπογραφές δικτύου επίθεσης και να εκχωρήσει ένα επίπεδο σοβαρότητας για κάθε πακέτο. Εάν τα επίπεδα σοβαρότητας είναι αρκετά υψηλά, τοποθετείται προειδοποιητικό μήνυμα ηλεκτρονικού ταχυδρομείου ή κυψελοειδής μήνυμα (sms) στα μέλη της ομάδας ασφαλείας, ώστε να μπορούν να διερευνήσουν περαιτέρω τη φύση της ανωμαλίας.

Τα IDS με βάση το δίκτυο έχουν γίνει δημοφιλή καθώς αυξάνεται το μέγεθος και η επισκεψιμότητα του Διαδικτύου. Τα IDS που μπορούν να ανιχνεύσουν τις ογκώδεις ποσότητες της δραστηριότητας δικτύου και να επισημάνουν με επιτυχία την ύποπτη μετάδοση είναι ευπρόσδεκτα στο πλαίσιο της βιομηχανίας ασφάλειας. Λόγω της εγγενούς ανασφάλειας των πρωτοκόλλων TCP / IP, έχει καταστεί επιτακτική ανάγκη να αναπτυχθούν σαρωτές, sniffers και άλλα εργαλεία ελέγχου και ανίχνευσης δικτύων για την αποφυγή παραβιάσεων της ασφάλειας που οφείλονται σε μια τέτοια κακόβουλη δραστηριότητα δικτύου, όπως:

- IP Spoofing
- denial-of-service attacks
- arp cache poisoning
- DNS name corruption
- man-in-the-middle attacks

Τα περισσότερα IDS που βασίζονται στο δίκτυο απαιτούν τη ρύθμιση της συσκευής δικτύου του κεντρικού συστήματος σε μη ελεγχόμενη λειτουργία, η οποία επιτρέπει στη συσκευή να συλλάβει κάθε πακέτο που μεταφέρεται στο δίκτυο.

3.3.2 HOST – BASED IDS (Συστήματα ανίχνευσης εισβολής με βάση τον κεντρικό υπολογιστή)

Ένα σύστημα ανίχνευσης εισβολής βασισμένο σε κεντρικό υπολογιστή (HIDS) είναι ένα σύστημα ανίχνευσης εισβολής που είναι σε θέση να παρακολουθεί και να αναλύει τα εσωτερικά ενός υπολογιστικού συστήματος καθώς και τα πακέτα δικτύου στις διασυνδέσεις του δικτύου του, παρόμοια με τον τρόπο που το κάνει ένα σύστημα ανίχνευσης εισβολής με βάση το δίκτυο (NIDS). Αυτός ήταν ο πρώτος τύπος

λογισμικού ανίχνευσης εισβολής που σχεδιάστηκε, με το αρχικό σύστημα στόχου να είναι ο κεντρικός υπολογιστής όπου η εξωτερική αλληλεπίδραση ήταν σπάνια.

Ένα αναγνωριστικό IDS που βασίζεται στον κεντρικό υπολογιστή είναι ικανό να παρακολουθεί όλα ή μέρη της δυναμικής συμπεριφοράς και την κατάσταση ενός συστήματος υπολογιστή, με βάση τον τρόπο με τον οποίο έχει διαμορφωθεί. Εκτός από δραστηριότητες όπως η δυναμική επιθεώρηση πακέτων δικτύου που στοχεύουν σε αυτόν τον συγκεκριμένο κεντρικό υπολογιστή (προαιρετική συνιστώσα με τις περισσότερες λύσεις λογισμικού που διατίθενται στο εμπόριο), ο HIDS ενδέχεται να εντοπίσει ποιο πρόγραμμα αποκτά πρόσβαση σε ποιους πόρους και ανακαλύπτει ότι για παράδειγμα ένας επεξεργαστής λέξεων έχει ξεκινήσει ξαφνικά και ανεξήγητα τη βάση δεδομένων κωδικού πρόσβασης συστήματος. Ομοίως, το HIDS μπορεί να εξετάσει την κατάσταση ενός συστήματος, τις αποθηκευμένες πληροφορίες του, είτε στη μνήμη RAM , στο σύστημα αρχείων, στα αρχεία καταγραφής ή αλλού και να ελέγξει ότι τα περιεχόμενα αυτών εμφανίζονται όπως αναμένεται, π.χ. δεν έχουν αλλάξει από εισβολείς.

Μπορεί κανείς να σκεφτεί ένα HIDS ως πράκτορα που παρακολουθεί αν οτιδήποτε ή οποιοσδήποτε, είτε εσωτερικός είτε εξωτερικός, έχει παρακάμψει την πολιτική ασφάλειας του συστήματος.

3.4 Μηχανισμοί ανίχνευσης και ανάλυσης επιθέσεων

Στον τομέα της Ανίχνευσης Επιθέσεων υπάρχουν τρεις βασικοί μηχανισμοί ανάλυσης των πληροφοριών, η ανίχνευση ανωμαλιών (anomaly detection), η ανίχνευση κατάχρησης (misuse detection) και η ανίχνευση βασισμένη σε προδιαγραφές (specification based detection). Στις παρακάτω παραγράφους θα δούμε μια περαιτέρω ανάλυση και εμβάθυνση των συγκεκριμένων μοντέλων.

- Συστήματα Ανίχνευσης Ανωμαλιών

Η ανίχνευση ανωμαλιών (anomaly detection) βασίζεται και στηρίζεται στη γενική υπόθεση ότι ένα πληροφοριακό σύστημα έχει κάποια συγκεκριμένη συμπεριφορά όταν βρίσκεται υπό φυσιολογικές συνθήκες, η οποία διαφοροποιείται όταν το σύστημα βρίσκεται σε κατάσταση επίθεσης. Με πιο απλά λόγια, η ανίχνευση ανωμαλιών επιχειρεί να εντοπίσει συμπεριφορές συστημάτων μη προβλεπόμενης δραστηριότητας, που συνήθως αποκλίνουν από τη κανονική και φυσιολογική τους λειτουργία. Εστιάζει στην κατασκευή προτύπων σχετικά με τη χρήση του συστήματος που παρακολουθείται, συνδυάζοντας διαφορετικές μετρικές και παρατηρώντας πιθανές σημαντικές αποκλίσεις. Ο αριθμός των διεργασιών που δημιουργούνται και εκτελούνται , ο αριθμός των συνδέσεων στο εκάστοτε δίκτυο και η συχνότητα εισαγωγής, είναι μερικές μόνο από τις μετρικές που χρησιμοποιούνται. Η δημιουργία του συγκεκριμένου μοντέλου θα πρέπει να περιέχει και να συγκρίνει τις καινούριες μετρικές που εισήλθαν με τις προηγούμενες μετρικές, οι οποίες βρίσκονται υπό συνθήκες κανονικής χρήσης του συστήματος. Τα κατώφλια (threshold) που καθορίζονται κατά τη διάρκεια της ρύθμισης ενός IDS, χρησιμοποιούνται από το σύστημα για να χαρακτηρίσουν τυχόν δραστηριότητες που περνούν τα παραπάνω κατώφλια σαν εισβολές.

- Συστήματα Ανίχνευσης Κατάχρησης

Τα συστήματα ανίχνευσης κατάχρησης (misuse detection) ψάχνουν και προσπαθούν να εντοπίσουν συγκεκριμένα πρότυπα χρήσης ή ακόμη και ακολουθίες γεγονότων που είναι είδη γνωστά από προηγούμενες απόπειρες εισβολής. Εξαιτίας αυτού του χαρακτηριστικού, το μοντέλο αυτό μπορεί να χαρακτηριστεί ως μία τεχνική βασισμένη στην εκ των προτέρων γνώση και είναι εφαρμόσιμή μόνο όταν υπάρχει ή μπορεί να κατασκευαστεί μία υπογραφή που να περιγράφει την επίθεση. Επιπρόσθετα τα συστήματα ανίχνευσης κατάχρησης έχουν πολλές λανθασμένες θετικές όπως και αρνητικές προειδοποιήσεις. Η ακρίβεια τέτοιων συστημάτων ανίχνευσης εξαρτάται κυρίως από την ακρίβεια των υπογραφών, οι οποίες πρέπει να είναι σαφείς. Συνεπώς όταν κάποιος εισβολέας επιτίθεται με άγνωστα για το σύστημα πρότυπα, όπως είναι η απουσία υπογραφής τότε προκύπτει μια λανθασμένη αρνητική προειδοποίηση. Αντιθέτως όταν ένα συμβάν ταιριάζει με μια υπογραφή επίθεσης αλλά δεν αποτελεί απειλή, τότε προκύπτει λανθασμένη θετική προειδοποίηση. Τα συστήματα ανίχνευσης κατάχρησης ενεργοποιούν πολύ λίγες λανθασμένες θετικές ενεργοποιήσεις το αντίθετο όμως γίνεται με τις αρνητικές που ενεργοποιούν πάρα πολλές.

- Συστήματα Ανίχνευσης Βασισμένα σε Προδιαγραφές

Η ανίχνευση Βασισμένη σε Προδιαγραφές έχει παρόμοια αντιμετώπιση με την ανίχνευση ανωμαλιών, αλλά αντί να εστιάζει στη δραστηριότητα του χρήστη, επικεντρώνεται στην αναμενόμενη συμπεριφορά του συστήματος. Όπως όλα τα συστήματα ανίχνευσης επιθέσεων έτσι και τα συστήματα βάσει προδιαγραφών μπορούν να παρουσιάσουν λανθασμένες αρνητικές προειδοποιήσεις. Για να έχει πλήρη αποτελεσματικότητα η ανίχνευση βασισμένη σε προδιαγραφές, ο αναλυτής πρέπει να καθορίσει τη συμπεριφορά του συστήματος για κάθε πιθανή κατάσταση και να κατασκευάσει ένα προφίλ για το σύστημα παρακολούθησης. Αφότου δημιουργηθεί το προφίλ κάθε ενέργεια του συστήματος συγκρίνεται με αυτό και κάθε απόκλισή του χαρακτηρίζεται εισβολή.

3.5 Χρησιμότητα IDS

Καθώς οι δικτυακές επιθέσεις έχουν αυξηθεί κατά πολύ τα τελευταία χρόνια τόσο σε πλήθος όσο και σε βαθμό επικινδυνότητας, τα IDS αποτελούν μία απαραίτητη προσθήκη στην πολιτική ασφάλειας κάθε οργανισμού.

Η Ανίχνευση Επιθέσεων επιτρέπει στους οργανισμούς να προστατέψουν τα συστήματά τους και τις πληροφορίες που βρίσκονται σε αυτά, από κινδύνους που προκύπτουν από την αυξημένη δικτυακή διασύνδεση μεταξύ των συστημάτων τους.

Υπάρχουν διάφοροι λόγοι για τους οποίους είναι απαραίτητη η χρήση των IDS:

- Για ανίχνευση επιθέσεων και άλλων παραβιάσεων ασφάλειας που δε ανιχνεύονται από άλλα μέτρα προστασίας. Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ένα ή περισσότερα συστήματα, όταν διάφορες, δημόσια γνωστές

αδυναμίες ασφάλειας των συστημάτων αυτών δεν έχουν διορθωθεί. Παρόλο που κάθε διαχειριστής πρέπει και μπορεί σχετικά εύκολα να διορθώνει τις αδυναμίες αυτές, υπάρχουν διάφοροι λόγοι για τους οποίους αυτό δεν συμβαίνει.

- ✓ Σε περιβάλλοντα με πολλά συστήματα, ο διαχειριστής τους συνήθως δεν έχει την δυνατότητα αλλά ούτε και τον χρόνο να ενημερώσει τα συστήματα που πρέπει, με νέες διορθώσεις των αδυναμιών ασφάλειάς τους.

- ✓ Οι χρήστες των συστημάτων κάνουν χρήση διάφορων λογισμικών που θεωρούνται επικίνδυνα, με την έννοια ότι μπορούν να προκαλέσουν τρύπες ασφάλειας σε ένα σύστημα.

- ✓ Τόσο οι διαχειριστές όσο και οι χρήστες κάνουν λάθη στην ρύθμιση και την χρήση των συστημάτων και των υπηρεσιών που προσφέρουν.

- ✓ Οι χρήστες χρησιμοποιούν μειωμένης ασφάλειας μηχανισμούς πρόσβασης στα συστήματα, όπως ατυχώς επιλεγμένα passwords.

Σε έναν ιδανικό κόσμο οι δημιουργοί λογισμικού θα μείωναν στο ελάχιστο τις αδυναμίες ασφάλειάς στα προϊόντα που διανέμουν και οι διαχειριστές θα ενημέρωναν και θα διόρθωναν τα συστήματά τους γρήγορα και αξιόπιστα. Στον πραγματικό όμως κόσμο αυτό σπάνια συμβαίνει, ενώ νέες αδυναμίες και ελαττώματα στην ασφάλεια συστημάτων, εμφανίζονται σε καθημερινή βάση.

Με την χρήση ενός IDS η προσπάθεια ή και η επιτυχία ενός επιτιθέμενου να παραβιάσει κάποιο σύστημα μέσω της εκμετάλλευσης μιας γνωστής αδυναμίας σε αυτό, θα γινόταν αντιληπτή. Επίσης με την βοήθεια του IDS, γνωστοποιείται η αδυναμία που οδήγησε στην παραβίαση του συστήματος και παράγονται χρήσιμα συμπεράσματα που βοηθούν στην αποκατάσταση του συστήματος και την διόρθωση της αδυναμίας, που οδήγησε στην παραβίασή του.

- ➢ Για την ανίχνευση αναγνωριστικών ενεργειών που προηγούνται μίας επίθεσης. Για την πραγματοποίηση μίας επίθεσης συνήθως υπάρχουν κάποια στάδια που προηγούνται αυτής. Ο επιτιθέμενος πρώτα εξετάζει τον υποψήφιο στόχο του, ώστε να συγκεντρώσει πληροφορίες για αυτόν και να εντοπίσει ένα σημείο εσόδου, το οποίο θα του επιτρέψει να πραγματοποιήσει την επίθεση με επιτυχία. Αυτό επιτυγχάνεται μέσω του Scanning. Δίχως την ύπαρξη ενός IDS, ο επιτιθέμενος είναι πολύ πιθανό να πραγματοποιήσει τις αναγνωριστικές του κινήσεις ανενόχλητος και χωρίς να γίνει αντιληπτός. Ένα IDS θα είχε την δυνατότητα να εντοπίσει τις κινήσεις αυτές του επιτιθέμενου και να πάρει κάποια μέτρα, όπως να καταγράψει το γεγονός, να ειδοποιήσει τους υπεύθυνους ασφάλειας για αυτό ή και να εμποδίσει τον επιτιθέμενο να τις ολοκληρώσει.

- ➢ Για την συγκέντρωση πληροφοριών που αφορούν επιθέσεις που πραγματοποιήθηκαν, οι οποίες θα βοηθήσουν στην αποκατάσταση των συστημάτων που παραβιάστηκαν και στην διόρθωση αδυναμιών και παραλήψεων στα ήδη

υπάρχοντα μέτρα ασφάλειας. Ακόμα και στην περίπτωση που ένα IDS δεν μπορεί να εμποδίσει μία επίθεση, μπορεί να συλλέξει διάφορες πληροφορίες και στοιχεία για αυτήν που θα χρησιμοποιηθούν τόσο για την αποκατάσταση του συστήματος και την διόρθωση των αδυναμιών ασφάλειάς του, όσο και για τον εντοπισμό του επιτιθέμενου και την ποινική δίωξή του.

- Για να αποτραπούν επίδοξοι επιτιθέμενοι, καθώς υπάρχει μεγαλύτερο ρίσκο να εντοπιστούν και να τιμωρηθούν. Όταν ο υποψήφιος επιτιθέμενος συνειδητοποιήσει ότι ένα δίκτυο ή ένα σύστημα προστατεύεται από ένα IDS, διστάζει να συνεχίσει την προσπάθειά του καθώς υπάρχουν περισσότερες πιθανότητες να γίνει αντιληπτός και να συλληφθεί

- Για αποτελεσματικότερη σχεδίαση και εφαρμογή πολιτικής ασφάλειας. Με την χρήση των IDSs συλλέγονται πληροφορίες και παρατηρούνται patterns από ενέργειες που πραγματοποιούνται καθημερινά εναντίον ενός δικτύου και των συστημάτων του, τα οποία μπορούν να βοηθήσουν στη σχεδίαση πιο αξιόπιστων μέτρων ασφάλειας, προσαρμοσμένων ώστε να αντιμετωπίζουν τα γεγονότα και τους κινδύνους που απειλούν το συγκεκριμένο δίκτυο, και να οδηγήσουν στην αποτελεσματικότερη προστασία του.

ΚΕΦΑΛΑΙΟ 4

Στο κεφάλαιο αυτό θα δούμε τα Honeypots.

Εικόνα 4.1 : Honeypot.
Πηγή: https://www.fidelissecurity.com/threatgeek/deception/honeypots/

4.1 Ορισμός honeypot

«Honeypot ονομάζεται ένας πόρος πληροφοριακών συστημάτων του οποίου η αξία έγκειται στην μη εξουσιοδοτημένη ή παράνομη χρήση του πόρου αυτού» [11]

Με πιο απλά λόγια το honeypot είναι ένα σύνολο πόρων το οποίο το εκθέτουμε στο δίκτυο έτσι ώστε να δελεάσουμε και να παρασύρουμε κακόβουλους

χρήστες με σκοπό να επιτεθούν σε αυτό, και εμείς με την σειρά μας να καταγράψουμε και να αναλύσουμε τις κινήσεις που αυτοί πραγματοποίησαν.

Η ιδέα του honeypot είναι σχετικά απλή. Ο πόρος αυτός δεν έχει καμία παραγωγική αξία για τον ιδιοκτήτη του όπως και κανένας νόμιμος χρήστης δεν έχει λόγο να αλληλεπιδράσει με αυτόν. Επομένως οποιαδήποτε προσπάθεια αλληλεπίδρασης με το honeypot θεωρείται κακόβουλη και τις πιο πολλές φορές πρόκειται για ανίχνευση, δικτυακή σάρωση ή επίθεση. Στις περιπτώσεις όμως που το honeypot πραγματοποιεί εξωτερική σύνδεση προς κάποιον ξένο διαδικτυακό πόρο τότε το σύστημα έχει κατά πάσα πιθανότητα καταληφθεί από κάποιον κακόβουλο χρήστη.

Τα Honeypots μπορούν να εγκατασταθούν οπουδήποτε. Πιο συχνά όμως τοποθετούνται εντός τοίχους προστασίας για καλύτερο έλεγχο. Κατά κάποιο τρόπο αποτελούν παραλλαγές των κλασικών συστημάτων ανίχνευσης εισβολών (IDS), αλλά δίνουν βάση περισσότερο στη συγκέντρωση πληροφοριών και εξαπάτησης.

Εγκαθίστανται με τέτοιο τρόπο ώστε να αποτελούν εύκολη λεία για τους επιτιθέμενους σε σχέση με τα πραγματικά συστήματα παραγωγής αλλά με μικρές τροποποιήσεις ώστε η δραστηριότητά τους να μπορέσει να ανιχνευτεί και να καταγραφεί. Η λειτουργία τους βασίζεται στην φιλοσοφία που λέει ότι αν κάποιος εισβολέας επιτεθεί σε ένα σύστημα μια φορά θα το επαναλάβει και άλλες φορές. Κατά την διάρκεια αυτών των επιθέσεων θα συγκεντρωθούν πρόσθετες πληροφορίες και επιπλέον προσπάθειες πρόσβασης στο σύστημα αρχείων και ασφαλείας θα παρακολουθηθούν και θα αποθηκευτούν.

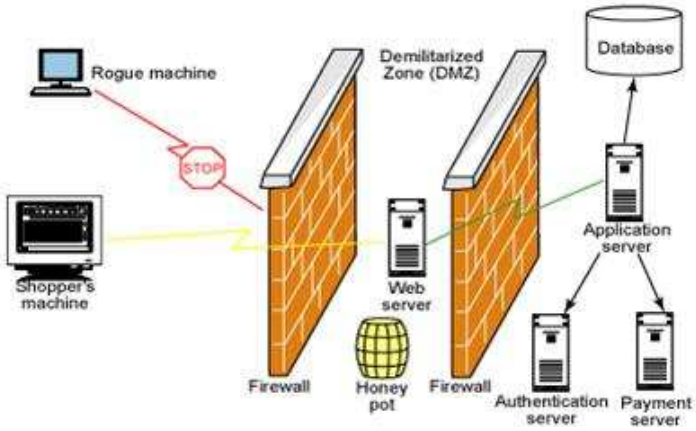
Οι κυριότεροι λόγοι για την εγκατάσταση ενός Honeypot είναι οι εξής:

- Εκμάθηση του τρόπου που οι εισβολείς προσπαθούν να αποκτήσουν πρόσβαση σε ένα σύστημα. Από την στιγμή που καταγράφεται η δραστηριότητα του εισβολέα, ο χρήστης μπορεί να μάθει τις μεθοδολογίες των εισβολών και έτσι να προστατέψει καλύτερα τα πραγματικά συστήματα παραγωγής.
- Συγκέντρωση πληροφοριών που σχετίζονται για την κατανόηση των κινήσεων και των κινήτρων των εισβολέων.

Η χρήση μεθόδων εξαπάτησης και παραπλάνησης των εισβολέων θεωρείται αποδεκτή στην χρήση των Honeypots, γεγονός που με την σειρά του καθορίζει κάποιες προδιαγραφές που πρέπει να τηρούνται.

- Το Honeypot πρέπει να φαίνεται όσο το δυνατόν πιο γενικό γίνεται. Για παράδειγμα αν χρησιμοποιούμε ένα λειτουργικό σύστημα της Microsoft θα πρέπει να μην φαίνεται ότι το σύστημα έχει τροποποιηθεί ή ότι θα πραγματοποιηθεί μία αποσύνδεση προτού οι εισβολείς κατορθώσουν να συγκεντρώσουν τον όγκο δεδομένων που θέλουν.
- Θέλει μεγάλη προσοχή στην κίνηση που επιτρέπεται στον εισβολέα να στείλει πίσω στο διαδίκτυο γιατί μπορεί εύκολα το σύστημά μας να γίνει σημείο εκκίνησης επιθέσεων εναντίον άλλων οντοτήτων. Για τον λόγο αυτό και τα Honeypot εγκαθίστανται εντός του τείχους προστασίας.
- Τα δεδομένα που θα έχει το Honeypot πρέπει να φαίνονται νόμιμα και πραγματικά ώστε οι εισβολείς να θεωρούν ότι πραγματοποίησαν το στόχο τους.

Παράλληλα, πρέπει να ληφθούν σοβαρά υπόψη κατά το σχεδιασμό και τη χρήση των Honeypot ότι τα δεδομένα που συγκεντρώνονται από αυτά δεν μπορούν να χρησιμοποιηθούν ως ποινικά τεκμήρια για άσκηση ποινικής δίωξης των εισβολέων. Όπως και το ότι οργανώσεις hacking συχνά στήνουν παγίδες εναντίον των Honeypots και πολλές φορές τα μετατρέπουν ενδεχομένως σε στόχο για εισβολείς.

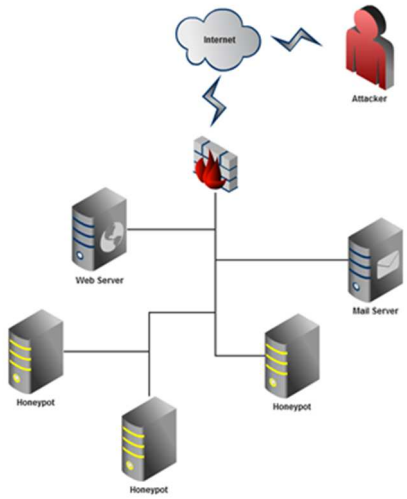


Εικόνα 4.2 : Τυπικό μοντέλο Honeypot εντός τείχους προστασίας.
Πηγή: https://www.biyanicolleges.org/honeypot-technology/

4.2 Τρόπος λειτουργίας της προσομοίωσης στα honeypots

Η δυνατότητα των honeypots να προσομοιώνουν διάφορα είδη λειτουργικών συστημάτων αλλά και δικτυακών συσκευών οφείλεται στη χρήση των λεγόμενων αποτυπωμάτων (fingerprints), δηλαδή μοναδικών αναγνωριστικών που χαρακτηρίζουν κάθε λειτουργικό σύστημα. Τα αποτυπώματα αυτά έχουν να κάνουν με τη στοίβα IP (IP stack) του κάθε λειτουργικού συστήματος και πώς αυτή έχει κατασκευαστεί. Για την ακρίβεια υπάρχουν οκτώ στον αριθμό παράμετροι του πρωτοκόλλου TCP/IP που δεν είναι σταθερές και αφήνεται στην ευχέρεια των προγραμματιστών του εκάστοτε λειτουργικού συστήματος να τις υλοποιήσουν δίνοντας διάφορες τιμές που εκείνοι επιλέγουν. Διαφορετικά λειτουργικά συστήματα ή και διαφορετικές εκδόσεις του ίδιου λειτουργικού συστήματος έχουν επομένως διαφορετικές τιμές σε αυτές τις παραμέτρους.

Όλες αυτές οι παράμετροι συνδυασμένες μαζί φτιάχνουν μια υπογραφή (signature) μεγέθους 67 bits, ή αλλιώς το αποτύπωμα του συγκεκριμένου λειτουργικού συστήματος. Μέσω αυτών των υπογραφών μπορεί να αναγνωριστεί το λειτουργικό σύστημα με το οποίο κάποιος έχει αλληλεπίδραση. Με αυτό τον τρόπο γίνεται για παράδειγμα η ανίχνευση του λειτουργικού συστήματος από το γνωστό δικτυακό εργαλείο nmap. Τα honeypots χρησιμοποιούν τον ίδιο μηχανισμό για να προσομοιώνουν διάφορα λειτουργικά συστήματα, οι τιμές των αποτυπωμάτων των οποίων είναι ήδη γνωστές. Πέρα από το λειτουργικό σύστημα,
πραγματοποιείται και η προσομοίωση διαφόρων δικτυακών υπηρεσιών. Αυτό γίνεται κατά κανόνα με τη χρήση διαφόρων σεναρίων εντολών (scripts) που η συμπεριφορά τους είναι ίδια με αυτή της αντίστοιχης πραγματικής υπηρεσίας.



Εικόνα 4.3 : Απεικόνιση της αρχιτεκτονικής ενός δικτύου που έχουν εγκατασταθεί τρία honeypots ανάμεσα στα πραγματικά συστήματα παραγωγής υπό επίθεση. Πηγή: Πτυχιακή Εργασία Ιωάννης Κονιάρης ''Ανάλυση Κυβερνοεπιθέσεων με honeypots μεσαίας και χαμηλής αλληλεπίδρασης''

4.3 Ιστορία των Honeypots

Στα τέλη του 20ου αιώνα δημοσιεύονται τα πρώτα άρθρα και επιστημονικά συγγράμματα τα οποία αποτέλεσαν τα θεμέλια για την ανάπτυξη των Honeypots. Η ιστορία των honeypots αρχίζει στα μέσα της δεκαετίας του '80 και παρουσιάζει μεγάλο ενδιαφέρον. Πολλοί στρατιωτικοί, επιχειρηματικοί και κυβερνητικοί οργανισμοί πραγματοποίησαν σημαντικές ερευνητικές και αναπτυξιακές δραστηριότητες. Ωστόσο, ελάχιστες πληροφορίες κοινοποιήθηκαν πριν το '90 και μόλις πρόσφατα αναπτύχθηκε λογισμικό και δημοσιεύθηκαν άρθρα για την συγκεκριμένη ιδέα. Δημοσιεύσεις σχετικές με γεγονότα, ιδέες και έννοιες έθεσαν τα θεμέλιά για την ανάπτυξη των honeypots στα τέλη του 20ου αιώνα.

Αρχικά ο αστρονόμος Clifford Stoll στο βιβλίο του ''The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage'' το 1989 διηγείται, πώς αντιλήφθηκε έναν επιτιθέμενο σε σύστημα της αστρονομικής κοινότητας κατά την διάρκεια της εργασίας του. Έδωσε όλη του την προσοχή στη συστηματική παρακολούθησή του και στην συγκέντρωση στοιχείων ώστε να μπορέσει να αναγνωρίσει την ταυτότητά του, προστατεύοντας συγχρόνως το σύστημά του. Ο Clifford δεν δημιούργησε honeypot αλλά χρησιμοποίησε παραγωγικά συστήματα της ακαδημαϊκής και ερευνητικής κοινότητας με στόχο να δελεάσει τον επιτιθέμενο, και το έκανε με τέτοιο τρόπο που προσέγγιζε την τεχνολογία των honeypots. Η ιδιαιτερότητα που έχει το βιβλίο του και επίσης η συμβολή του στην ιστορία των honeypots έγκειται στις ιδέες τις οποίες ανέπτυξε.

Στη συνέχεια ο Bill Cheswick στο άρθρο του ‘’An Evening with Berferd in Which a Cracker Is Lured, Endured, and Studied’’ το 1992 περιγράφει τη δημιουργία ενός συστήματος που εξειδικεύεται στην προσέλκυση επιτιθέμενων. Στην ουσία αυτό το άρθρο αποτελεί την πρώτη τεκμηριωμένη παρουσίαση ενός honeypot. Ο Cheswick αναφέρεται διεξοδικά στη μελέτη της δραστηριότητας του επιτιθέμενου και στις συνέπειες της δραστηριότητάς του στο σύστημα και όχι στην ανάλυση τεχνολογικών θεμάτων που αφορούν το honeypot.

Οι εξελίξεις συνεχίστηκαν με έντονο ρυθμό στη διάρκεια της δεκαετίας του ‘90 όσο αφορά στο πεδίο της ασφάλειας των δικτύων. Εκτός από το θεωρητικό υπόβαθρο το 1997 ήρθε και η πρώτη σχετική υλοποίηση με το Deception toolkit (DTK) του Fred Cohen. Θεωρητικά αυτό σήμερα είναι το πρώτο Honeypot.

Στην ουσία είναι μία συλλογή από Perl scripts σχεδιασμένα για Unix συστήματα που προσομοιώνουν μία πληθώρα αδυναμιών. Η ιδέα του deception toolkit είναι η παραπλάνηση του επιτιθέμενου. Πιο συγκεκριμένα μπορεί να στηθεί με το toolkit ένα σύστημα το οποίο θα δείχνει να έχει πολλές γνωστές αδυναμίες. Αυτό επιτυγχάνεται με την αποστολή εξόδου προς τον επιτιθέμενο μου μοιάζει σαν αληθινή. Έτσι π.χ. όταν ο επιτιθέμενος στέλνει το send mail exploit, το DTK απαντάει κανονικά και έτσι ο επιτιθέμενος νομίζει πως η επίθεση ήταν επιτυχής. Με αυτό τον τρόπο από την μία οι διαχειριστές καταφέρνουν να καταγράψουν την επίθεση και να απαντήσουν προτού το σύστημα δεχτεί επίθεση που πραγματικά θα λειτουργήσει και από την άλλη ο επιτιθέμενος χάνει πολύτιμο χρόνο.

Η πρώτη εμπορική λύση στο χώρο των honeypots με το Cybercopsting ήρθε το 1998-1999, το οποίο μπορούσε να προσομοιώσει πολλές διαφορετικές δικτυακές συσκευές. Την ίδια περίοδο δημιουργήθηκε και το NetFacade, και αυτό προσομοίωνε δικτυακές συσκευές αλλά σε μεγαλύτερη κλίμακα. Παρόλο που δεν σημείωσε μεγάλη επιτυχία, άφησε πίσω του ένα debugging δικτυακό εργαλείο το οποίο ουσιαστικά αποτέλεσε την βάση για την μετέπειτα δημιουργία του Snort IDS. Το BackOfficer Friendly ήταν το πρώτο Windows honeypot το οποίο διανεμόταν δωρεάν αν και δεν ήταν και πολύ λειτουργικό, δημοσιοποιώντας σε μεγάλο βαθμό την μέχρι τότε άγνωστη τεχνολογία των honeypots.

Ιδιαίτερα σημαντική υπήρξε η πραγμάτωση από τον Lance Spitzen του Honeynet Project το 1999. Ο Spitzner συντέλεσε ώστε να συγκροτηθεί μία ομάδα επαγγελματιών της ασφάλειας, οι οποίοι επικεντρώθηκαν στην συγκέντρωση και την μελέτη εξαιρετικά χρήσιμων πληροφοριών με στόχο τη γνωστοποίησή τους στους ενδιαφερόμενους. Το βιβλίο τους ‘’Know Your Enemy: Learning about Security Threats’’ δημοσιεύθηκε το 2001, το οποίο αναφέρεται στη ερευνά τους και τα αποτελέσματα της.

Η ερευνητική δραστηριότητα στα πλαίσια του Honeynet Project υποστηρίχθηκε από ένα βελτιωμένο και εξελιγμένο είδος honeypot το honeynet, το οποίο αποτελεί ένα δίκτυο από honeypots. Τον 21ο αιώνα η ανάπτυξη των honeypots συνεχίζεται με γνώμονα τις εξειδικευμένες γνώσεις που αποκτούνται σταδιακά από την μελέτη των επιτιθέμενων όπως π.χ. το 2003 με το Snort-Inline, το Sebek κ.α. καθώς και την εξέλιξη των honeypots σε προηγμένα συστήματα από απλά εργαλεία που ήταν.

4.4 Κατηγοριοποίηση των honeypots

Υπάρχουν διαφόρων ειδών honeypots τα οποία και διαφέρουν στην υλοποίηση και τον τρόπο χρήσης τους. Τα honeypots γενικά μπορούν να κατηγοριοποιηθούν (classification) με χρήση τριών κριτηρίων.

Τα κριτήρια κατηγοριοποίησης των honeypots είναι:

- ✓ Στόχος και σκοπός χρήσης του honeypot.
- ✓ Επιτρεπτό επίπεδο αλληλεπίδρασης μεταξύ του εισβολέα και του honeypot.
- ✓ Αρχιτεκτονική υλοποίησης του honeypot.

4.4.1 Κατηγοριοποίηση με βάση τον στόχο και τον σκοπό χρήσης του honeypot.

Τα honeypots μπορούν να διαχωριστούν σε δύο κατηγορίες ανάλογα με τον σκοπό και το κίνητρο πίσω από την υλοποίηση τους. Έχουμε έτσι τα ερευνητικά (research) honeypots και τα honeypots παραγωγής (production).

Τα πρώτα είναι συστήματα με κύριο στόχο να καταγράφουν δεδομένα και πληροφορίες ώστε να αυξάνεται η γνώση των ειδικών ασφαλείας σχετικά με τον τρόπο δράσης της κοινότητας των κακόβουλων χρηστών (blackhat community). Η βασική χρήση τους είναι η προσομοίωση συχνά χρησιμοποιούμενων υπηρεσιών ώστε να δελεάσουν διάφορους εισβολείς (hackers) να επιτεθούν εναντίον τους. Συνήθως υλοποιούνται σε ερευνητικά κέντρα, πανεπιστήμια, κυβερνητικές ή στρατιωτικές υπηρεσίες και οργανισμούς με σχετικό ερευνητικό αντικείμενο. Δεν έχουν άμεση σχέση με την ασφάλεια του ίδιου του οργανισμού από τον οποίο υλοποιούνται και περισσότερο χρησιμοποιούνται για την καταγραφή γεγονότων ώστε να βοηθήσουν στη γενικότερη αντιμετώπιση των διαδικτυακών απειλών, προβλέποντας επιθέσεις και κάνοντας γνωστούς τους τρόπους λειτουργίας των εισβολέων.

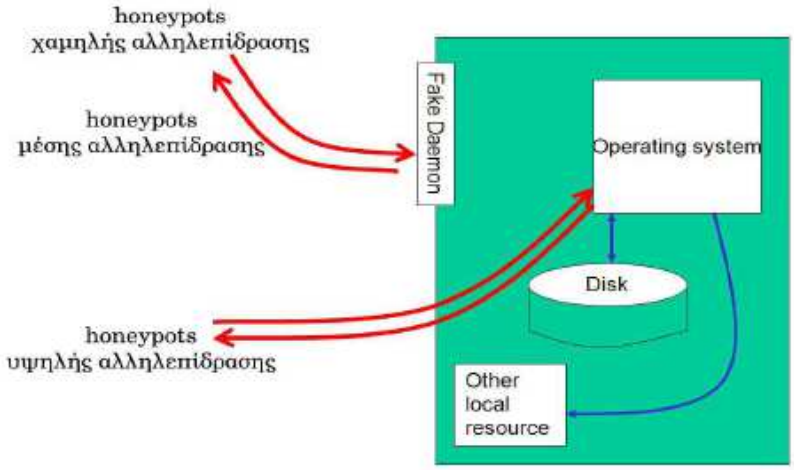
Τα δεύτερα είναι honeypots που βρίσκονται μέσα στο δίκτυο μιας εταιρείας ή ενός οργανισμού με σκοπό να προστατέψουν το συγκεκριμένο δίκτυο. Αυτό γίνεται εφικτό δημιουργώντας ψεύτικα αντίγραφα των συστημάτων που χρησιμοποιεί ο οργανισμός και δελεάζοντας εισβολείς να επιτεθούν σε αυτά, ώστε οι διαχειριστές του δικτύου να αποκτήσουν πληροφορίες για τα ρίσκα των πραγματικών συστημάτων που έχουν υπό την εποπτεία τους. Τα δεδομένα των honeypots παραγωγής αναλύονται και ορισμένες πραγματικές υπηρεσίες ή διακομιστές υπηρεσιών μπορούν να προστατευθούν αποτελεσματικότερα.

Θα πρέπει να ειπωθεί ξανά πως τα honeypots δεν έχουν κάποια αξία ως συστήματα πρόληψης ή παρεμπόδισης εισβολών (intrusion prevention systems). Αυτό που κάνουν είναι απλά να καταγράφουν την κίνηση που ανιχνεύουν και να συγκεντρώνουν δεδομένα. Αποτελεί ξεχωριστό τομέα της ασφάλειας το πώς ένας οργανισμός προστατεύει συνολικά το δίκτυο του με σωστό τρόπο. Παρόλα αυτά, τα honeypots και ειδικότερα τα honeypots παραγωγής, συνδράμουν σημαντικά στην αντιμετώπιση των δικτυακών απειλών όταν χρησιμοποιούνται σε συνδυασμό με άλλα αντίμετρα ασφαλείας όπως τα συστήματα ανίχνευσης επιθέσεων (IDS) και τείχη προστασίας (firewalls).

4.4.2 Κατηγοριοποίηση με βάση το επιτρεπτό επίπεδο αλληλεπίδρασης μεταξύ του εισβολέα και του honeypot.

Πρόκειται για τη βασικότερη διάκριση μεταξύ των συστημάτων honeypots. Εφόσον τα honeypots προσφέρονται ως δόλωμα και πρόκειται να δεχτούν επιθέσεις, το επίπεδο αλληλεπίδρασης με τον εκάστοτε εισβολέα είναι ένα πολύ σημαντικό κριτήριο του είδους που θα επιλεγεί για εγκατάσταση σε ένα δίκτυο. Διαφορετικά επιτρεπτά επίπεδα αλληλεπίδρασης προσφέρουν και διαφορετικές δυνατότητες, ενώ κάθε τύπος honeypot έχει τα ανάλογα θετικά και αρνητικά χαρακτηριστικά του.

Με βάση το κριτήριο αυτό τα honeypots χωρίζονται σε τρεις κατηγορίες: τα honeypots χαμηλής αλληλεπίδρασης (low-interaction), μεσαίας αλληλεπίδρασης (medium-interaction) και υψηλής αλληλεπίδρασης (high-interaction). Πέρα από το διαχωρισμό που επιτελούν, οι κατηγορίες αυτές αντικατοπτρίζουν και το αντίστοιχο ρίσκο που προσθέτει στο δίκτυο η ενσωμάτωση ενός τέτοιου συστήματος.



Εικόνα 4.4 : Επίπεδα αλληλεπίδρασης honeypots.
Πηγή: Διπλωματική Εργασία Τσιρεπλή Ισμήνη ‘’Honeypots & Honeyd’’

4.4.2.1 Honeypots χαμηλής αλληλεπίδρασης (low-interaction)

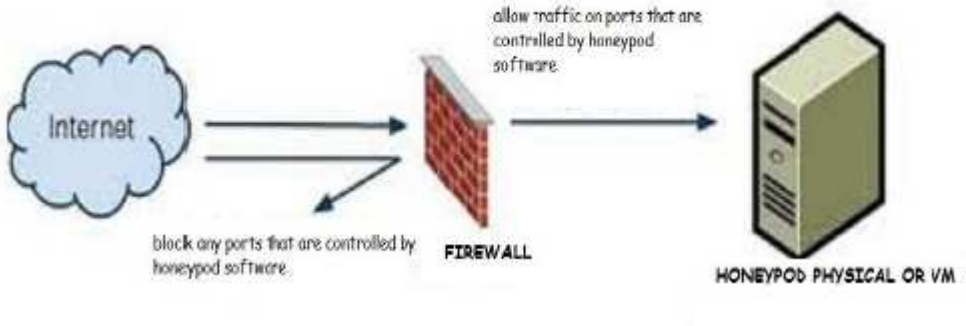
Τα honeypots χαμηλής αλληλεπίδρασης πήραν το όνομά τους λόγο της περιορισμένης αλληλεπίδρασης που μπορεί να έχει ένας επιτιθέμενος ή κάποιο κακόβουλο λογισμικό με το σύστημα. Προσομοιώνουν μόνο τμήματα ενός λειτουργικού συστήματος, δηλαδή αδυναμίες και υπηρεσίες. Για τον λόγο αυτό ο επιτιθέμενος δεν μπορεί να αποκτήσει πλήρη πρόσβαση στο λειτουργικό σύστημα και να εκμεταλλευτεί το λογισμικό για επιπλέον δικτυακές επιθέσεις. Ας πάρουμε σαν παράδειγμα την HTTP υπηρεσία που σε ένα χαμηλής αλληλεπίδρασης honeypot θα υποστήριζε τις εντολές που είναι απαραίτητες μόνο για την αναγνώριση μία επίθεσης.

Επομένως τα honeypots χαμηλής αλληλεπίδρασης έχουν περιορισμένες δυνατότητες αλλά χρησιμεύουν στο να συλλέγουν πληροφορίες για υψηλότερο επίπεδο, όπως για προγράμματα παρακολούθησης δικτύου ή για δραστηριότητες των worms. Επίσης μπορούν να χρησιμοποιηθούν για την λήψη αντιμέτρων εναντίον ιών τύπου worms ή για την ανάλυση δραστηριοτήτων αποστολέων ανεπιθύμητης αλληλογραφίας.

Τα honeypot αυτά συνήθως είναι γραμμένα σε γλώσσες σεναρίου (script based), και αυτές τις γλώσσες χρησιμοποιούν και στην αλληλεπίδραση που έχουν με τον επιτιθέμενο. Η εγκατάστασή τους και η συντήρησή τους είναι εύκολη και δεν απαιτούνται μεγάλοι υπολογιστικοί πόροι για την λειτουργία τους. Επιπρόσθετα η χρήση τους είναι απλή, ο κίνδυνος παραβίασης τους είναι ελάχιστος και ο όγκος δεδομένων που παράγουν για ανάλυση είναι σχετικά μικρός. Αποτελούν την ιδανική λύση για κάποιον αρχάριο χρήστη που θέλει να γνωρίσει την λειτουργικότητα των honeypots.

Τα χαμηλής αλληλεπίδρασης honeypot έχουν το κακό ότι με τις περιορισμένες δυνατότητες που έχουν μπορούν να θέσουν υποψίες στους εισβολείς ότι δεν αντιμετωπίζουν ένα πραγματικό σύστημα, ενώ ο μικρός παραγόμενος όγκος δεδομένων αυτομάτως σημαίνει και μικρότερη καταγραφή πληροφοριών σχετικά με τις επιθέσεις οπότε και μικρότερη εκπαιδευτική αξία.

Για παράδειγμα φτιάχνουμε ένα honeypot που προσομοιώνει έναν τυπικό εξυπηρετητή Unix που εκτελεί κάποιες υπηρεσίες όπως FTP και Telnet. Ο επιτιθέμενος θα μπορούσε να εκτελέσει το Telnet προς τον υποτιθέμενο εξυπηρετητή, να αποκτήσει ένα banner που να δηλώνει την κατάσταση του λειτουργικού συστήματος καθώς και μία προτροπή για είσοδο, και να προσπαθεί να εισέλθει στο σύστημα. Το honeypot μας θα συγκεντρώσει όλες αυτές τις προσπάθειες αλλά αφού δεν υπάρχει πραγματικό σύστημα η αλληλεπίδραση του εισβολέα θα παραμείνει σε προσπάθειες σύνδεσης.



Εικόνα 4.5 : Χαμηλής αλληλεπίδρασης honeypots.
Πηγή: Διπλωματική Εργασία Τσιρεπλή Ισμήνη ‘’Honeypots & Honeyd’’

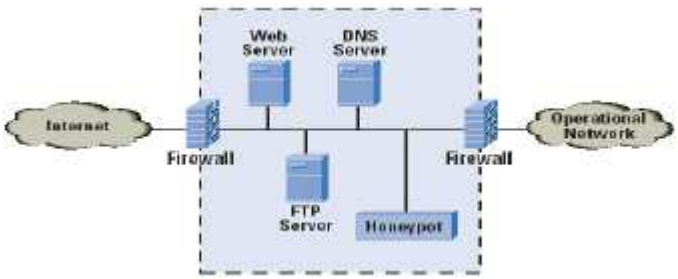
4.4.2.2 Honeypots υψηλής αλληλεπίδρασης (high-interaction)

Τα honeypots υψηλής αλληλεπίδρασης προσφέρουν ένα πραγματικό λειτουργικό σύστημα στους εισβολείς σε αντίθεση με τα άλλα honeypots. Αυτό τους επιτρέπει να έχουν από περιορισμένη έως και ολοκληρωτική πρόσβαση στο honeypot ανάλογα με το είδος επίθεσης που θα εξαπολύσουν και την αδυναμία του honeypot που θα εκμεταλλευτούν οι επιτιθέμενοι. Αποτελούνται από φυσικούς υπολογιστές με υπηρεσίες ευπαθείς ή μη, οι οποίοι τοποθετούνται μέσα σε ένα δίκτυο χωρίς να εκτελούν προσομοίωση. Επομένως ο εισβολέας επιτίθεται και εισέρχεται κατευθείαν στο λειτουργικό σύστημα του υπολογιστή που εκτελεί χρέη honeypot.

Ο κυριότερος σκοπός αυτών των honeypots είναι να βοηθήσουν τους υπεύθυνους έτσι ώστε να μάθουν τους στόχους των επιτιθέμενων και να διδαχτούν από αυτούς για να μπορέσουν να προστατέψουν τα πραγματικά τους συστήματα αποτελεσματικότερα. Αυτό μπορεί να επιτευχθεί με παρακολούθηση του εισβολέα σε πραγματικό χρόνο και ανάλυση των αρχείων καταγραφής. Για παράδειγμα, οι περισσότεροι εισβολείς που καταλαμβάνουν τέτοια συστήματα τα χρησιμοποιούν για δικούς τους σκοπούς που συνήθως είναι η εγκατάσταση και λειτουργία διακομιστών Internet Relay Chat. Οι διαχειριστές όμως των honeypots μπορούν να παρεμβάλλονται στα κανάλια επικοινωνίας και να καταγράφουν τις συνομιλίες των κακόβουλων χρηστών επιτυγχάνοντας έτσι την συγκέντρωση δεδομένων ή ακόμα και την αποτροπή επικείμενων επιθέσεων σε άλλα συστήματα εντός του δικτύου που έχουν στην εποπτεία τους.

Εκτός από τα πλεονεκτήματα που αναφέραμε τα honeypots υψηλής αλληλεπίδρασης έχουν και μειονεκτήματα. Το μεγαλύτερο μειονέκτημα που έχουν είναι αυτό του μεγάλου ρίσκου, και αυτό επειδή πρόκειται για πραγματικά συστήματα ένας εισβολέας μπορεί να τα χρησιμοποιήσει ως ενδιάμεσα συστήματα ώστε να μπορέσει να επιτεθεί σε άλλους υπολογιστές του δικτύου που είναι παραγωγικοί. Για το λόγο αυτό θα πρέπει να προηγείται προσεκτικός σχεδιασμός της αρχιτεκτονικής του δικτύου καθώς και ακριβής τοποθέτηση ενός τέτοιου honeypot. Επίσης αυτό θα πρέπει πάντα να γίνεται σε συνδυασμό με υποστηρικτικές και απομονωτικές συσκευές όπως είναι τα τείχη προστασίας.

Σε αυτή την κατηγορία των honeypots ανήκουν τα honeynets και το Symantec Decoy Server.



Εικόνα 4.6 : Υψηλής αλληλεπίδρασης honeypots.
Πηγή: http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_7-4/dos_figure_6.gif

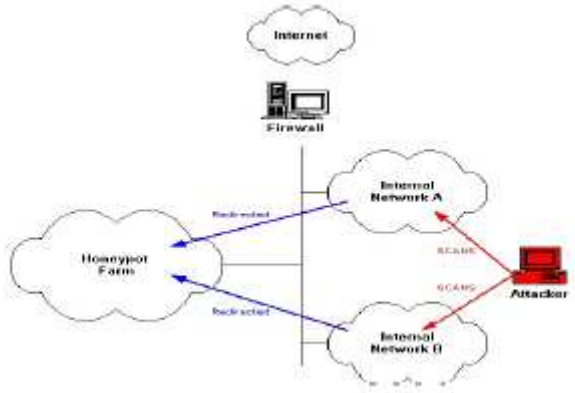
4.4.2.3 Honeypots μεσαίας αλληλεπίδρασης (medium-interaction)

Τα honeypots μεσαίας αλληλεπίδρασης διαθέτουν περισσότερους τρόπους αλληλεπίδρασης μεταξύ εισβολέα και συστήματος. Επίσης έχουν την δυνατότητα να ανταποκρίνονται στις εντολές του επιτιθέμενου με ψεύτικες πληροφορίες με τέτοιο τρόπο ‘ώστε ο επιτιθέμενος να νομίζει ότι επρόκειτο για μια πραγματική δικτυακή υπηρεσία.

Σε αυτή την κατηγορία ανήκουν και τα malware honeypots που έχουν ως στόχο την σκόπιμη μόλυνση τους από κακόβουλο λογισμικό έτσι ώστε να μπορέσει να καταγραφεί και να αναλυθεί το τοπικό αντίγραφο από ειδικούς. Στην περίπτωση αυτή το ρόλο των επιτιθέμενων τον παίρνει κάποιο κακόβουλο λογισμικό που είναι ήδη εγκατεστημένο σε άλλους υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο και προσπαθεί να διαδώσει τον εαυτό του. Το honeypots σύστημα μπορεί εύκολα να προσομοιώνει υπηρεσίες οι οποίες αποτελούν συχνό στόχο τέτοιου λογισμικού καθώς και να απαντά με τέτοιο τρόπο που να ξεγελά τους επιτιθέμενους και να νομίζουν ότι πρόκειται για ευπαθές σύστημα.

Επειδή τα honeypots μεσαίας αλληλεπίδρασης μπορούν να δεχτούν δεδομένα ως είσοδο καθώς και να επιτρέψουν την πρόσβαση σε ένα ελεγχόμενο περιβάλλον εντός του αληθινού λειτουργικού συστήματος θεωρούνται αυξημένου ρίσκου honeypots. Το ρίσκο όμως δεν είναι τόσο μεγάλο αν οι χρήστες του τηρούν ορισμένες σωστές πρακτικές σε συνδυασμό με κάποιους απαραίτητους ελέγχους του λογισμικού για τυχόν ευπάθειες.

Σε αυτή την κατηγορία των honeypots ανήκουν το Kippo, το Dionaea και το HoneyBOT.



Εικόνα 4.7 : Μεσαίας αλληλεπίδρασης honeypots.
Πηγή: https://slideplayer.com/slide/6955486/

4.4.3 Κατηγοριοποίηση με βάση την υλοποίηση

Τα honeypots με βάση την υλοποίησή τους, χωρίζονται σε δύο κατηγορίες:

1. Φυσικά
2. Εικονικά

4.4.3.1 Φυσικά honeypots

Τα φυσικά honeypots είναι εγκαταστάσεις λειτουργικών συστημάτων σε υπολογιστές οι οποίοι επιβλέπονται. Η εκτέλεση τους γίνεται σε πραγματικά συστήματα τα οποία έχουν και την δικιά τους IP διεύθυνση. Επίσης μπορούν να τρέξουν σε πολλά και διάφορα λειτουργικά συστήματα όπως είναι τα Linux, Windows, Unix, Mac Os και άλλα.

Η εγκατάστασή τους είναι εύκολη και μπορεί να γίνει σε οποιοδήποτε λειτουργικό σύστημα χωρίς περιορισμούς. Ωστόσο τα συστήματα αυτά όπως και όλα έχουν και κάποια μειονεκτήματα από τα οποία το σοβαρότερο είναι ότι σε έναν υπολογιστή μπορεί να εγκατασταθεί μόνο ένα λειτουργικό σύστημα, με αποτέλεσμα την ανάγκη ανακατανομής των υπολογιστικών πόρων που χρησιμοποιούνται. Επιπρόσθετα η επανεγκατάσταση ενός τέτοιου συστήματος το οποίο έχει δεχθεί επίθεση είναι χρονοβόρα και μπορεί να προκαλεί και προβλήματα ακόμα και αν έχουν ληφθεί αντίγραφα ασφαλείας. Ακόμη απαιτείτε η μη αυτόματη πρόσβαση ώστε να διασφαλιστεί η λειτουργία μιας εγκατάστασης χωρίς να εμποδιστεί από τον επιτιθέμενο. Δεδομένου ότι οι εισβολείς μπορούν εύκολα να εντοπίσουν οποιαδήποτε αλλαγή στο λειτουργικό σύστημα του honeypot η παρακολούθησή του πρέπει να γίνεται μόνο από εξωτερικούς μηχανισμούς.

4.4.3.2 Εικονικά honeypots

Τα εικονικά honeypots είναι συστήματα που εγκαθίστανται και λειτουργούν εικονικά πάνω σε κάποιο άλλο κεντρικό λειτουργικό σύστημα.

Αυτά τα honeypots προσφέρουν πολλά πλεονεκτήματα. Το φιλοξενούμενο λειτουργικό σύστημα μπορεί να είναι τελείως διαφορετικό από το κεντρικό λειτουργικό ανάλογα με την τεχνική εικονικής διαμόρφωσης που θα ακολουθηθεί. Τα εικονικά συστήματα μπορούν να εγκατασταθούν παράλληλα σε έναν υπολογιστή και σε πολλές περιπτώσεις μπορούν να συνυπάρχουν πολλά και διαφορετικά λειτουργικά συστήματα. Μπορούν να γίνουν στόχος επίθεσης τα εικονικά honeypots χωρίς όμως να κινδυνεύουν τα κεντρικά συστήματα που τα φιλοξενούν. Η κατάσταση του εικονικού honeypot μπορεί να καταγράφεται από τον διαχειριστή του συστήματος οποιαδήποτε στιγμή, οπότε μπορεί πιο εύκολα να καταγράφει και τις κινήσεις του επιτιθέμενου προς το honeypot. Επίσης με τα εικονικά honeypots είναι πολύ πιο εύκολη η επανεγκατάσταση τους αφού χρειάζεται μόνο η ρύθμιση των εικονικών κόμβων από τον διαχειριστή του συστήματος.

Όπως είναι φυσικό το κύριο λειτουργικό σύστημα του υπολογιστή πρέπει να παραμένει κρυφό από τον επιτιθέμενο και να μην είναι ευάλωτο. Αυτό επιτυγχάνεται με την προσάρτηση του κύριου λειτουργικού συστήματος σε ξεχωριστό επίπεδο διασύνδεσης του δικτύου ή αλλιώς με σύνδεση με σειριακό καλώδιο στο οποίο έχει πρόσβαση μόνο ο διαχειριστής του honeypot.

Το κυριότερο μειονέκτημα των εικονικών honeypot είναι η έλλειψη ακρίβειας του επιπέδου εικονικοποίησης που με την σειρά του κάνει τον εισβολέα να μπορεί να καταλάβει αν πρόκειται για πραγματικό ή μη σύστημα. Από την άλλη όμως επειδή σήμερα οι υπηρεσίες παροχής Διαδικτύου χρησιμοποιούν τεχνικές εικονικοποίησης για να βελτιώσουν την απόδοση των διακομιστών του, το

μειονέκτημα μπορεί να θεωρηθεί και πλεονέκτημα γιατί μπερδεύει τους επιτιθέμενους και δεν μπορούν να καταλάβουν αν τελικά πρόκειται για εικονικό honeypot.

ΚΕΦΑΛΑΙΟ 5

Τα honeypots συμβάλουν ιδιαίτερα στην Ασφάλεια Υπολογιστικών Συστημάτων και αυτό το επιτυγχάνουν με το να καλύπτουν τα κενά ασφαλείας που προκύπτουν από τα τείχη προστασίας αλλά και από τα Συστήματα Ανίχνευσης Παρείσφρησης. Σε αυτό το κεφάλαιο θα αναλυθούν τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης των honeypots.

5.1 Πλεονεκτήματα της χρήσης των honeypots

- ✓ Χαμηλή ανάγκη πόρων: όπως έχουμε είδη πει παραπάνω τα περισσότερα honeypots έχουν χαμηλές απαιτήσεις πόρων. Για παράδειγμα τεράστια εικονικά δίκτυα μπορούν να δημιουργηθούν από το honeyd.

- ✓ Απλότητα: Τα πιο πολλά εργαλεία δεν χρησιμοποιούν πολύπλοκους και υψηλούς σε κατανάλωση πόρων αλγορίθμους άλλων τεχνολογιών, οπότε είναι απλά και δυναμικά.

- ✓ Ανακάλυψη νέων απειλών και μείωση των false negatives: Μπορούν να ανιχνεύουν νέα είδη απειλών και επιθέσεων τα honeypots. Οποιαδήποτε δραστηριότητα στο honeypot καταγράφεται σαν ανωμαλία.

- ✓ False positives: Τα αυξημένα false positives είναι ένα πρόβλημα σε παρόμοιες τεχνολογίες. Όμως επειδή οποιαδήποτε δραστηριότητα ή επικοινωνία με το honeypot θεωρείται κακόβουλη ο αριθμός των false positives μειώνεται στο ελάχιστο.

- ✓ Μικρή ποσότητα όγκου δεδομένων: Ο όγκος των δεδομένων που καταγράφεται από τα honeypots είναι μικρός σε μέγεθος οπότε και πιο εύκολα διαχειρίσιμος. Αυτό οφείλεται στο ότι τα honeypots μελετούν μόνο την κίνηση προς αυτά και δεν λαμβάνουν υπόψη άλλες δικτυακές κινήσεις.

- ✓ Κρυπτογράφηση: Το honeypot θα καταγράψει ακόμη και μια επίθεση που είναι κρυπτογραφημένη.

- ✓ Εσωτερικές απειλές: Σε οργανισμούς που έχουν αυξημένη πιθανότητα τέτοιων ειδών απειλών αποτελούν μια πολύ καλή λύση τα honeypots και honeytokens.

5.2 Μειονεκτήματα της χρήσης των honeypots

- ✓ Ρίσκο: Αν και στις πιο πολλές περιπτώσεις το ζητούμενο είναι να καταληφθεί το μηχάνημα από τους επιτιθέμενους, υπάρχει και ο κίνδυνος να χρησιμοποιηθεί το μηχάνημα ως πλατφόρμα επίθεσης προς άλλα δίκτυα. Αυτό αποτελεί και το βασικότερο μειονέκτημα των honeypots.

- ✓ Μικρή ποσότητα όγκου δεδομένων: Παρόλο που το αναφέραμε και πιο πάνω σαν πλεονέκτημα υπάρχουν περιπτώσεις που μπορούμε να πούμε πως είναι μειονέκτημα. Μία από αυτές είναι όταν χρειαζόμαστε μια πιο αναλυτική εικόνα στο τι έχει συμβεί σε μία δραστηριότητα και αυτό δεν είναι δυνατό.

- ✓ Τεκμηρίωση: Τα περισσότερα εργαλεία έχουν χαμηλού επιπέδου τεκμηρίωση. Αυτό συνεπάγεται με την μειωμένη ενασχόληση των χρηστών με τέτοιου είδους τεχνολογίες και προγράμματα.

- ✓ Fingerprinting και crackers: Σε πολλές περιπτώσεις αν ένας επιτιθέμενος έχει αρκετή εμπειρία που δεν είναι λίγοι αυτή που έχουν μπορεί να καταλάβει εύκολα πως πρόκειται για ψεύτικο δίκτυο και όχι πραγματικό.

ΚΕΦΑΛΑΙΟ 6

Στο κεφάλαιο αυτό θα δούμε και θα αναλύσουμε τα διάφορα honeypots που υπάρχουν. Αυτό θα το κάνουμε αφού πρώτα τα κατηγοριοποιήσουμε βάσει της αλληλεπίδρασης που έχουν.

6.1 Honeypots χαμηλής αλληλεπίδρασης

6.1.1 Dionaea

Το Dionaea είναι ένα honeypot χαμηλής αλληλεπίδρασης και έχει ως σκοπό του την απόκτηση αντιγράφων κακόβουλου λογισμικού, αυτό το επιτυγχάνει με την εξομοίωση διάφορων πρωτοκόλλων. Πολλοί το ονομάζουν απόγονο του honeypot Nepenthes. Για περισσότερη ευελιξία και ευκολία έχει ενσωματωμένη ως γλώσσα σεναρίου την python, για τον εντοπισμό κώδικα κελύφους χρησιμοποιεί τη βιβλιοθήκη libemu, καθώς υποστηρίζει και την τεχνολογία IPV6 και TLS (Transport Layer Security).

Τα πρωτόκολλα που υποστηρίζονται από το Dionaea είναι τα εξής:

- **SMB (Server Message Protocol)**: Είναι το κύριο πρωτόκολλο του Dionaea. Λειτουργεί σε επίπεδο εφαρμογής καθώς είναι δικτυακό πρωτόκολλο και καθορίζει σε ένα δίκτυο την πρόσβαση σε αρχεία, θύρες και εκτυπωτές. Το πρωτόκολλο αυτό χρησιμοποιείται πιο πολύ σε υπολογιστές που τρέχουν

Microsoft Windows λειτουργικό και είναι ευρέος διαδεδομένο με την ονομασία CIFS (Common Internet File System). Το Dionaea χρησιμοποιεί το πρωτόκολλο SMB γιατί είναι ο πιο ελκυστικό στόχος για worms. Τέλος η θύρα που χρησιμοποιείται για αυτό το πρωτόκολλο είναι η 445.

- **HTTP και HTTPS**: Ενώ το Dionaea δεν χρησιμοποιεί και δεν αναλύει τα δεδομένα που μαζεύει από αυτά τα πρωτόκολλα, παρόλα αυτά χρησιμοποιεί την 80 θύρα για το HTTP και την 443 για το HTTPS πρωτόκολλο.
- **FTP (File Transfer Protocol)**: Το Dionaea χρησιμοποιεί για την δημιουργία καταλόγων καθώς και για τη αποστολή και λήψη αρχείων έναν βασικό διακομιστή FTP στη θύρα 21.
- **TFTP (Trivial File Transfer Protocol):** Το Dionaea έχει έναν TFTP διακομιστή για τον διαμοιρασμό αρχείων στη θύρα 69.
- **MSSQL (Microsoft SQL Server)**: Το Dionaea υποστηρίζει το πρωτόκολλο TDS (Tabular Data Stream) το οποίο χρησιμοποιείται από το MSSQL. Παρότι δεν υπάρχει βάση δεδομένων το Dionaea χρησιμοποιεί τη θύρα 1433 για την σύνδεση στον SQL διακομιστή και την εκτέλεση επερωτήσεων.
- **MySQL**: Το Dionaea μέσω της θύρας 3306 προωθεί όλες τις επερωτήσεις προς τη MySQL βάση δεδομένων σε μία τοπική SQLite βάση δεδομένων.
- **SIP**: Το Dionaea για χρήση VoIP (Voice Over IP) χρησιμοποιεί το πρωτόκολλο SIP και δεν συνδέεται με κάποιον εξωτερικό διακομιστή VoIP όπως κάνουν άλλα VoIP honeypots. Επίσης ο χρήστης μπορεί να επιλέξει όνομα χρήστη SIP και κωδικό πρόσβασης καθώς υποστηρίζει πολλαπλές συνεδρίες SIP και καναλιών RTP. Τέλος όλα τα δεδομένα καταγράφονται σε SQLite βάση δεδομένων.

6.1.2 Back Officer friendly (BOF)

Το Back Officer friendly είναι ένα πρόγραμμα το οποίο εκτελείται κατά βάση σε συστήματα με λειτουργικό Windows. Έχει παρόμοια λειτουργία με το honeypot Specter αλλά είναι πιο απλό στην χρήση του.

Το BOF προσομοιώνει κάποιες βασικές υπηρεσίες όπως είναι οι HTTP, FTP, TELNET, POP3, SMTP, BackOrifice και IMAP. Επικεντρώνεται στην καταγραφή οποιασδήποτε σύνδεσης ή ακόμα και προσπάθειας στις ανοιχτές TCP θύρες. Επίσης έχει και την επιλογή faking replies με την οποία απαντά στις συνδέσεις των επιτιθέμενων με χρήση συμβολοσειρών, όμως δεν είναι παραμετροποιήσιμη από τον χρήστη.

Το πρόγραμμα αυτό μπορεί να παρομοιαστεί με έναν οικιακό συναγερμό επειδή μπορεί να παρακολουθήσει μόνο ένα συγκεκριμένο αριθμό θυρών οι οποίες όμως δέχονται πολύ συχνά επιθέσεις.

Το BOF δεν ενδείκνυται για δίκτυα είναι πιο πολύ για οικιακή χρήση. Αν και η διανομή του έχει σταματήσει από το επίσημο site της NFR διανέμεται ακόμα δωρεάν από την προσωπική σελίδα του Lance Spitzner.

6.1.3 Specter

Το Specter όπως αναφέραμε και παραπάνω έχει παρόμοια λειτουργία με το BOF αλλά με πολύ μεγαλύτερη λειτουργικότητα και περισσότερη προσομοίωση υπηρεσιών.

Το honeypot αυτό τρέχει σε επίπεδο εφαρμογής σε Windows 2000 Service Pack 2 ή Windows XP Service Pack 1 και ελέγχει αυτόματα online για εβδομαδιαίες ενημερώσεις προγραμμάτων. Εκλύει 14 διαφορετικά λειτουργικά συστήματα, συμπεριλαμβανομένων των Windows 98, Windows NT, Windows 2000, Windows XP, MacOS, καθώς και πλήθος παραλλαγών Unix. Προσφέρει επίσης 14 διαφορετικές υπηρεσίες TCP: SMTP, FTP, telnet, finger, POP3, IMAP4, HTTP, SSH, DNS, SUN-RPC, μια μόνο προσαρμόσιμη θύρα και μερικούς Trojans (NetBus, Back Orifice 2000 και SubSeven). Όπως φαίνεται στον παρακάτω πίνακα, το Specter ταξινομεί επτά από αυτά ως παγίδες και επτά ως εξομοιωμένες υπηρεσίες.

Παγίδες	**Υπηρεσίες**
DNS	FTP
IMAPv4	SMTP
SSH	HTTP
SUN-RPC	Telnet
Sub-7	Finger
BOK2	POP3
Generic	NetBus

Πίνακας 6.1 : Παγίδες και υπηρεσίες Specter

Οι παγίδες είναι απλά θύρες που ακούν και καταγράφουν ανιχνευτές και τερματίζουν τυχόν προσπάθειες σύνδεσης. Η γενική παγίδα είναι οποιαδήποτε θύρα TCP που επιλέγετε, αλλά μπορεί να είναι μόνο μία, η οποία είναι λίγο περιοριστική. Οι υπηρεσίες θα προσπαθήσουν να μιμηθούν υπηρεσίες που θα υπήρχαν στο OS που επιλέγετε. Για παράδειγμα, εάν επιλέξετε το λειτουργικό σύστημα των Windows, θα μιμηθούν τις υπηρεσίες IIS, FTP, Exchange Server κ.ο.κ. Οι επτά υπηρεσίες μπορούν να προσαρμοστούν ελαφρώς προσθέτοντας το δικό σας περιεχόμενο, οθόνες banner και λογαριασμούς χρηστών. Ορισμένες από τις εξομοιωμένες υπηρεσίες, όπως το telnet, προσφέρουν στον απομακρυσμένο χάκερ μια προσπάθεια σύνδεσης (αν και ο χάκερ δεν μπαίνει ποτέ στη σύνδεση). Άλλοι, όπως το HTTP και το POP3, επιτρέπουν περισσότερη αλληλεπίδραση, συμπεριλαμβανομένης της σύνδεσης και της

απόκτησης περιεχομένου. Στο κάτω μέρος, το SPECTER δεν μπορεί να μιμηθεί τίποτα εκτός από αυτές τις 14 θύρες TCP και δεν ακούει τις θύρες UDP ή το ICMP.

Το Specter διαθέτει πολλές μοναδικές λειτουργίες, όπως σημειωτές, προσαρμοσμένο περιεχόμενο, ψεύτικα αρχεία κωδικών πρόσβασης και ευφυΐα εντοπισμού. Το πιο ενδιαφέρον χαρακτηριστικό του Specter είναι η ικανότητά του να επισημάνει τον απομακρυσμένο χάκερ. Το Specter μπορεί να δημιουργήσει δυναμικά περισσότερα από 100 διαφορετικά εκτελέσιμα προγράμματα και μπορεί να αφήσει έως και 32 δείκτες σε ένα σύστημα χάκερ. Θεωρητικά, οι εν λόγω δείκτες θα μπορούσαν να χρησιμοποιηθούν από τις υπηρεσίες επιβολής του νόμου για τη δίωξη των χάκερ (αν και δεν νομίζω ότι έχουν χρησιμοποιηθεί με αυτόν τον τρόπο ακόμα).

Το Specter βρίσκεται στην κορυφή της κατηγορίας του στην περιοχή του ενσωματωμένου περιεχομένου. Περιέχει έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου, ιστοσελίδες και ακόμη και ψεύτικους λογαριασμούς χρηστών και κωδικούς πρόσβασης. Είναι επίσης το μόνο honeypot που γνωρίζω ότι δημιουργεί δυναμικά πλαστό περιεχόμενο. Και όταν κάνει την εβδομαδιαία ενημέρωση του προγράμματος, μπορεί να αλλάξει το περιεχόμενό του, τα τρωτά σημεία και τους δείκτες. Μπορεί να δημιουργήσει ψεύτικα αρχεία κωδικού πρόσβασης των Windows με διαφορετικά επίπεδα δυσκολίας για να κατεβάσουν οι χάκερ.

Οι επιλογές αυτόματης νοημοσύνης του Specter περιλαμβάνουν το finger, το traceroute, τη σάρωση των λιμένων, το whois, τις αναζητήσεις DNS και ακόμη και το banner grabbing. Αυτό επιτρέπει, κατόπιν επιλογής του διαχειριστή, για τους απομακρυσμένους χάκερ να ανιχνευθούν και να αποτυπωθούν δακτυλικά αποτυπώματα ενώ κάνουν το ίδιο. Αυτή η λειτουργία πρέπει να χρησιμοποιείται με προσοχή, καθώς η επιθετική απάντηση ενδέχεται να προειδοποιήσει τον εισβολέα.

6.1.4 Honeyd

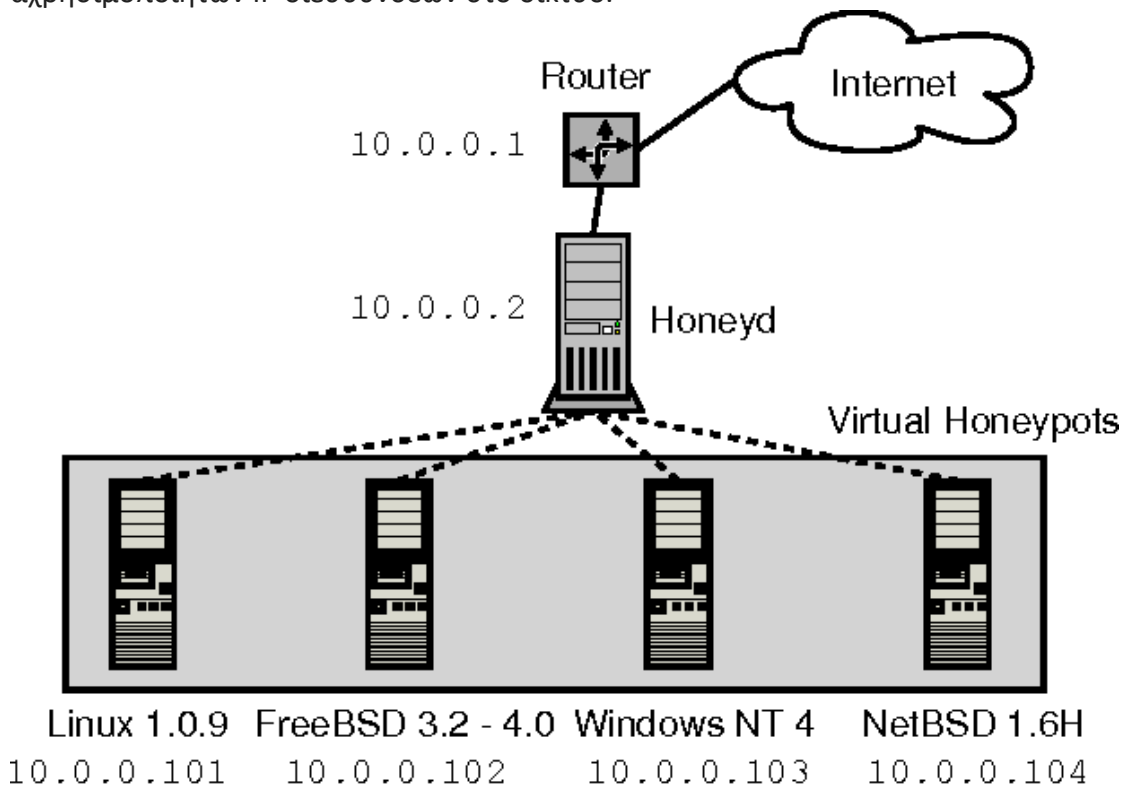
Το honeyd είναι ένα ανοιχτού κώδικα, χαμηλής διαδραστικότητας εικονικό honeypot που επιτρέπει την δημιουργία εικονικών συστημάτων σε ένα δίκτυο[1]. Τα εικονικά αυτά συστήματα μπορούν να προσομοιώσουν διαφόρων τύπων λειτουργικά συστήματα καθώς και ένα μεγάλο αριθμό από υπηρεσίες που αυτά παρέχουν. Δημιουργός του είναι ο Niels Provos.

Το honeyd μπορεί να προσομοιώσει έως 216 εικονικά συστήματα [2] . Κάθε ένα από αυτά τα εικονικά συστήματα μπορεί να προσομοιώσει υπηρεσίες που βασίζονται στα πρωτόκολλα SMTP, FTP, HTTP κλπ. Η χρήση του μπορεί να γίνει:

- Για ερευνητικούς σκοπούς, όπως, για παράδειγμα, για εξόρυξη δεδομένων χρησιμοποιώντας τα στοιχεία που συλλέγονται από τις διάφορες επιθέσεις.

- Για αντιπερισπασμό απέναντι σε κακόβουλους χάκερ , επιχειρώντας να "κρύψει" αληθινά συστήματα ανάμεσα σε εικονικά. Ο επιτιθέμενος θα αναγκαστεί να σπαταλήσει χρόνο, χρησιμοποιώντας εναλλακτικά μέσα για την ανακάλυψη των αληθινών συστημάτων. Αυτή η διαδικασία μπορεί να δώσει στον διαχειριστή του δικτύου τον απαραίτητο χρόνο για να λάβει τα κατάλληλα αντίμετρα. εφ' όσον διαπιστώσει ύποπτη κίνηση στο δίκτυο.

Η προσομοίωση των συστημάτων γίνεται χρησιμοποιώντας την τεχνική ARP spoofing. Το honeyd μπορεί να ρυθμιστεί ώστε να καλύπτει το εύρος όλων των αχρησιμοποίητων IP διευθύνσεων στο δίκτυο.



Εικόνα 6.1 : Το Honeyd λαμβάνει κυκλοφορία για τα εικονικά honeypots μέσω δρομολογητή ή Proxy ARP.
Πηγή:
https://pdfs.semanticscholar.org/3124/456d251e3657746de4c34472224f5b2d8efe.pdf

6.1.5 HoneyC

Το HoneyC είναι ένα Client honeypot το οποίο αναπτύχθηκα από τον Christian Seifert το 2006 με σκοπό να αναγνωρίσει τους κακόβουλους εξυπηρετητές στο Διαδίκτυο. Χρησιμοποιεί προσομοιωμένους clients και όχι πλήρες λειτουργικό με πλήρες client για την αναζήτηση απαντήσεων που απαιτούνται να αναλυθούν από έναν εξυπηρετητή. Επίσης το HoneyC είναι επεκτάσιμο καθώς μπορεί να χρησιμοποιήσει διάφορους clients ως επισκέπτες όπως και συστήματα αναζήτησης και ανάλυσης αλγορίθμων.

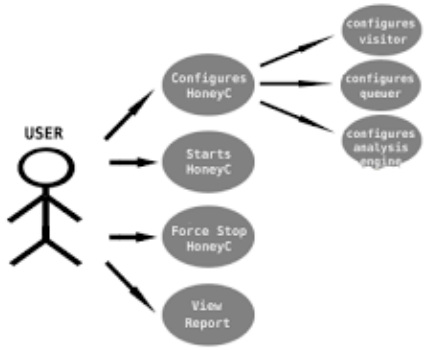
Τα συστατικά που αποτελούν το HoneyC είναι τρία, ο Visitor, ο Queuer και η Analysis Engine.

1. Ο Visitor είναι το συστατικό που ευθύνεται για την επικοινωνία με τον εξυπηρετητή. Η λειτουργία του είναι απλή κάνει αίτημα προς τον εξυπηρετητή και όταν λάβει την απόκρισή του την επεξεργάζεται.
2. Ο Queuer είναι αυτός που αναλαμβάνει να δημιουργήσει μια ουρά από εξυπηρετητές ώστε να μπορεί ο Visitor να αλληλεπιδρά με αυτούς. Αυτό το

επιτυγχάνει με διάφορους αλγορίθμους όπως είναι η ανίχνευση στο διαδίκτυο, η ενσωμάτωση μέσω μηχανής αναζήτησης και άλλα.

3. Η Analysis Engine είναι αυτή που θα εκτιμήσει αν παραβιάστηκε κάποιος μηχανισμός ασφαλείας κατά το διάστημα αλληλεπίδρασης του Visitor με τον εξυπηρετητή.

Πρόσθετες λειτουργικές μονάδες επιτρέπονται από αυτά τα στοιχεία αν χρειαστούν για ανάγκες που πιθανόν να προκύψουν. Μέσω εντολών ανακατεύθυνσης (pipes) γίνεται η σύνδεση ανάμεσα στις μονάδες αυτές και τους μηχανισμούς αίτησης και απόκρισης ώστε να είναι ανεξάρτητη η λειτουργία τους.



Εικόνα 6.2 : Αλληλεπίδραση χρήστη με HoneyC.
Πηγή: https://projects.honeynet.org/honeyc/wiki/AboutHoneyC

6.1.6 Monkey – Spider

Το Monkey – Spider είναι και αυτό ένα client honeypot το οποίο ανιχνεύει ιστοσελίδες ώστε να υποδείξει ενδεχόμενες απειλές σε clients διαδικτυακούς. Το ξεκίνησε ο Ali Ikinci ως μεταπτυχιακή διατριβή το Μάιο του 2007 και από τότε διανέμεται δωρεάν από την GPLv3 άδεια. Το Μάρτιο του 2009 εκδόθηκε η τελευταία έκδοση που είναι η 2.0.

Μέσω προκαθορισμένων υπογραφών κακόβουλου λογισμικού, όπως και εμπορικών antivirus και antispyware το Monkey – Spider μπορεί να ανιχνεύσει οποιοδήποτε είδος κακόβουλου λογισμικού όπως trojan, virus, spyware, worm, phishing, adware και hoax. Επίσης μέσω αυτοματοποιημένων τεχνικών προσομοίωσης και ανάλυσης κακόβουλου λογισμικού είναι σε θέση να ανιχνεύσει και άγνωστες απειλές.

Αυτό το honeypot είναι κατάλληλο για οργανισμούς, εταιρίες και ερευνητές ασφαλείας που επιθυμούν την ανακάλυψη των απειλών στις εταιρικές τους ιστοσελίδες αυτοματοποιημένα. Επιπρόσθετα μπορεί να χρησιμοποιηθεί και για forums ή κοινοτικές ιστοσελίδες όπου οι χρήστες μπορούν να ανεβάσουν περιεχόμενο.

Στην αρχή υπήρχε μία διεπαφή χρήστη αλλά επείδη δεν ήταν λειτουργική εγκαταλείφθηκε και τώρα υπάρχει μόνο διασύνδεση μέσω γραμμής εντολών. Επίσης εγκαταλείφθηκε και η αναζήτηση μέσω Google που στην αρχή υπήρχε. Το Monkey – Spider δεν υποστηρίζει την ανάλυση επισυναπτόμενων αρχείων. Τέλος για την αυθεντικοποίηση των αιτήσεων απαιτεί μοναδικά αναγνωριστικά για κάθε χρήστη Microsoft ή Yahoo τα οποία ανακτά από τα επίσημα site της Microsoft και της Yahoo αντίστοιχα.

Το Monkey – Spider εγκαθίσταται σε λειτουργικό Linux και απαιτούνται τα εργαλεία awk, sed, wget, unzip, grep και Python 2.5 τουλάχιστον. Εκτός από τα εργαλεία αυτά χρειάζονται και τα παρακάτω πακέτα:

- ✓ Διαδικτυακός ανιχνευτής Heritrix
- ✓ PostgreSQL βάση δεδομένων που απαιτεί αυθεντικοποίηση με κωδικό για διασύνδεση πάνω από το δίκτυο
- ✓ ClamAV anti – virus ανιχνευτή
- ✓ Την Python διεπαφή PyGreSql για την PostgreSQL βάση δεδομένων
- ✓ SOAPpy για τη σύνδεση στη μηχανή αναζήτησης Microsoft
- ✓ pYsearch για τη σύνδεση στη μηχανή αναζήτησης Yahoo

Σε hardware οι ελάχιστες απαιτήσεις είναι επεξεργαστής Pentium και μνήμη ram 128MB.

Ανάλογα με το ερευνητικό ενδιαφέρον του χρήστη τρέχουν και τα κατάλληλα script του Monkey – Spider τα οποία μπορούν να τρέξουν και ανεξάρτητα το ένα με το άλλο.

6.1.7 PhoneyC

Το PhoneyC είναι ένα εικονικό client honeypot, που σημαίνει ότι δεν είναι μια πραγματική εφαρμογή, αλλά μάλλον ένας εξομοιωμένος client. Με τη χρήση δυναμικής ανάλυσης, το PhoneyC είναι σε θέση να αφαιρέσει την εμπλοκή από πολλές κακόβουλες σελίδες. Επιπλέον, το PhoneyC προσομοιώνει συγκεκριμένες ευπάθειες για τον εντοπισμό του φορέα επίθεσης. Το PhoneyC είναι ένα αρθρωτό πλαίσιο που επιτρέπει τη μελέτη κακόβουλων σελίδων HTTP και κατανοεί σύγχρονες ευπάθειες και τεχνικές εισβολέων.

Τα πιο βασικά χαρακτηριστικά του PhoneyC περιλαμβάνουν:

- Ερμηνεία χρήσιμων ετικετών HTML για απομακρυσμένους συνδέσμους
  - ✓ hrefs, imgs, κλπ ...
  - ✓ iframes, πλαίσια, κλπ
- Ερμηνεία των γλωσσών scripting
  - ✓ javascript (μέσω spidermonkey)
  - ✓ υποστηρίζει την απομάκρυνση, απομακρυσμένες πηγές δέσμης ενεργειών
- Ενότητες "ευπάθειας ActiveX" για ανίχνευση εκμετάλλευσης
- Ανίχνευση και ανάλυση κελύφους (μέσω libemu)
- Ανίχνευση σωρού

Το PhoneyC διανέμεται δωρεάν υπό την άδεια της GNU μιας και αποτελεί λογισμικό ανοιχτού κώδικα.

6.1.8 SpyBye

Το SpyBye είναι ένα εργαλείο που βοηθά τους διαχειριστές ιστοσελίδων να καθορίσουν εάν οι ιστοσελίδες τους φιλοξενούν προγράμματα ή λειτουργίες που μπορούν να μολύνουν τους επισκέπτες με κακόβουλα προγράμματα. Λειτουργεί ως διακομιστής μεσολάβησης HTTP και παρακολουθεί όλες τις αιτήσεις του προγράμματος περιήγησης. Το SpyBye χρησιμοποιεί μερικούς απλούς κανόνες για να καθορίσει εάν οι ενσωματωμένοι σύνδεσμοι στην ιστοσελίδα σας είναι επιβλαβείς, άγνωστοι ή ίσως ακόμη και επικίνδυνοι.

Το SpyBye λειτουργεί ως διακομιστής μεσολάβησης και παίρνει για να δει όλες τις ανακτήσεις ιστού που κάνει ο περιηγητής σας. Εφαρμόζει πολύ απλούς κανόνες σε κάθε διεύθυνση URL που λαμβάνεται ως αποτέλεσμα της φόρτωσης μιας ιστοσελίδας. Αυτοί οι κανόνες μας επιτρέπουν να ταξινομήσουμε μια διεύθυνση URL σε τρεις κατηγορίες: αβλαβείς, άγνωστες ή επικίνδυνες. Παρόλο που υπάρχει μεγάλο περιθώριο σφάλματος, οι κατηγορίες επιτρέπουν σε έναν κύριο ιστού να εξετάσει τις διευθύνσεις URL και να καθορίσει εάν πρέπει να είναι εκεί ή όχι. Εάν βλέπετε ότι μια διεύθυνση URL έχει παραληφθεί που δεν το περιμένατε, είναι μια καλή ένδειξη ότι έχει παραβιαστεί.

Το SpyBye δεν σας προστατεύει από το να εκμεταλλευτείτε τον εαυτό σας. Προσπαθεί να λάβει εύλογες προφυλάξεις για να αποφύγει τη μόλυνση κατά τη χρήση του. Ωστόσο, στην ιδανική περίπτωση, θα εκτελέσετε το πρόγραμμα περιήγησης σε μια εικονική μηχανή και θα επανέλθετε σε ένα καθαρό στιγμιότυπο όταν τελειώσετε. Σε έχω προειδοποιήσει. Το σημερινό κακόβουλο λογισμικό είναι ικανό να καταστήσει τον υπολογιστή σας ακατάλληλο - και να αδειάσει τους τραπεζικούς λογαριασμούς σας! Αυτό το λογισμικό είναι δική μου δουλειά ως άτομο και δεν συνδέεται με την Google ή δεν υποστηρίζεται από το πρόγραμμα StopBadware. Αυτό το λογισμικό παρέχεται από τον συντάκτη `` όπως είναι '' και οποιαδήποτε ρητή ή σιωπηρή εγγύηση, συμπεριλαμβανομένων, αλλά όχι περιοριστικά, των σιωπηρών εγγυήσεων εμπορευσιμότητας και καταλληλότητας για συγκεκριμένο σκοπό αποποιούνται. Σε καμία περίπτωση ο συγγραφέας δεν ευθύνεται για οποιεσδήποτε άμεσες, έμμεσες, παρεπόμενες, ειδικές, παραδειγματικές ή επακόλουθες ζημίες (συμπεριλαμβανομένης, ενδεικτικά, της προμήθειας υποκατάστατων αγαθών ή υπηρεσιών, απώλειας χρήσης, δεδομένων ή κερδών ή διακοπής λειτουργίας) που προκλήθηκε εντούτοις και σε οποιαδήποτε θεωρία ευθύνης, είτε με σύμβαση, αντικειμενική ευθύνη ή αδίκημα (συμπεριλαμβανομένης της αμέλειας ή άλλως) που προκύπτει με οποιονδήποτε τρόπο από τη χρήση αυτού του λογισμικού, ακόμη και αν έχει ενημερωθεί για την πιθανότητα τέτοιας ζημίας.

Το SpyBye αποτελεί και αυτό όπως και τα άλλα honeypots λογισμικό ανοιχτού κώδικα και διανέμεται δωρεάν υπό την άδεια της BSD και GPL.

6.1.9 LaBrea

Το LaBrea αναλαμβάνει τις μη χρησιμοποιούμενες διευθύνσεις IP και δημιουργεί εικονικούς διακομιστές ελκυστικούς για worms, hackers και άλλους χρήστες του Διαδικτύου. Το πρόγραμμα απαντά στις προσπάθειες σύνδεσης με τέτοιο τρόπο ώστε το μηχάνημα στο άλλο άκρο να «κολλάει», μερικές φορές για πολύ μεγάλο χρονικό διάστημα, από αυτό βγήκε και το όνομα sticky honeypot που το λένε αλλιώς το LaBrea.

Η τελευταία έκδοση του LaBrea είναι συμβατό με FreeBSD, Linux, Solaris και Windows (98/2K).

6.1.10 Nepenthes

Το Nepenthes είναι ένα Honeypot χαμηλής αλληλεπίδρασης, το οποίο εξομοιώνει γνωστά τρωτά σημεία και συλλαμβάνει worms καθώς προσπαθούν να το μολύνουν. Ενώ ο τρόπος λειτουργίας του Nepenthes σημαίνει ότι δεν θα εντοπίσει τους επιτιθέμενους που προσπαθούν να εκμεταλλευτούν άγνωστα τρωτά σημεία, μας επιτρέπει να εντοπίζουμε νέους τρόπους εκμετάλλευσης γνωστών τρωτών σημείων.

Το honeypot αυτό έχει την ικανότητα να αυτοματοποιεί τη διαδικασία ανάλυσης υποβάλλοντας σε διάφορα sandboxes καθένα από τα δυαδικά αρχεία που συλλέγει. Έτσι επιτυγχάνεται η καλύτερη ανάλυση από τους αναλυτές. Υπάρχουν όμως και φορές που η διαδικασία υποβολής δεν λειτουργεί όπως αναμένεται.

6.1.11 Thug

Οι κακόβουλες ιστοσελίδες για να ανιχνευτούν και εντοπιστούν, έχουν την ανάγκη ενός προσομοιωτή, ο οποίος να μπορεί να καθορίζει τη συμπεριφορά ενός διαδικτυακού φυλλομετρητή. Ο Angelo Dell' Aera κατάφερε να αναπτύξει αυτή ακριβώς την εφαρμογή. Το Thug λοιπόν είναι ένα client Honeypot χαμηλής αλληλεπίδρασης, που καλύπτει τις ποιο πάνω προϋποθέσεις. Διαθέτει το δικό του Docyment Object Model, (DOM) και χρησιμοποιεί, γι' αυτό το σκοπό τη μηχανή Google V8 Java Script.

Μέσω της χρήσης του Abstract syntax tree και της βιβλιοθήκης ανάλυσης κελύφους Libemu, καθώς και για την αντιμετώπιση των ευπαθειών και των δυνατοτήτων της στατικής και δυναμικής ανάλυσης, χρησιμοποιούνται τα στοιχεία ελέγχου Active X, τα οποία είναι και τα σημαντικότερα χαρακτηριστικά του. Η διανομή του είναι ελεύθερη με την άδεια της GNU, η αποτύπωσή του δε είναι σε Python.

6.1.12 Tiny

Το Tiny είναι ένα απλό honeypot που βασίζεται σε ανακατευθύνσεις του iptables και του listener xinetd. Ακούει σε κάθε θύρα TCP που δεν χρησιμοποιείται αυτή τη στιγμή, καταγράφοντας όλη τη δραστηριότητα και παρέχοντας κάποια ανατροφοδότηση στον εισβολέα. Οι ανταποκριτές γράφονται εξ ολοκλήρου στο Perl και παρέχουν αρκετή αλληλεπίδραση για να ξεγελάσουν τα πιο αυτοματοποιημένα

εργαλεία επίθεσης, καθώς και αρκετούς ανθρώπους, τουλάχιστον για λίγο. Με τα κατάλληλα όρια (προεπιλογή), η thp μπορεί να διαμένει στους οικοδεσπότες παραγωγής με αμελητέα επίδραση στην απόδοση.

6.1.13 Amun

Το Amun ήταν το πρώτο honeypot χαμηλής αλληλεπίδρασης που βασίζεται σε python, ακολουθώντας τις έννοιες του Nepenthes, αλλά επεκτείνοντας το με πιο εξελιγμένη εξομοίωση και ευκολότερη συντήρηση. Είναι ένα λογισμικό ανοιχτού κώδικα και διανέμεται δωρεάν από την GNU. Παρακάτω ακολουθεί μία σύντομη λίστα με τα πιο σημαντικά στοιχεία της Amun.

- Kernel Amun
- Χειριστής Αίτησης Amun
- Μονάδες ευπάθειας
- Αναλυτής Shellcode
- Λήψη στοιχείων
- Ενότητες υποβολής
- Ενότητες καταγραφής

6.1.14 Glastopf

Το Glastopf είναι ένα honeypot με χαμηλή αλληλεπίδραση, ικανό να εξομοιώνει χιλιάδες ευπάθειες για τη συλλογή δεδομένων από επιθέσεις που στοχεύουν σε εφαρμογές ιστού. Η αρχή πίσω από αυτό είναι πολύ απλή: απάντηση στην επίθεση χρησιμοποιώντας την απάντηση που ο εισβολέας αναμένει από την προσπάθειά του να εκμεταλλευτεί την εφαρμογή Ιστού. Παρέχουμε μια επισκόπηση των επιθέσεων σε εφαρμογές ιστού, περιγράφουμε παραδείγματα που συλλέχθηκαν με το Glastopf και συζητήσαμε πιθανές χρήσεις των δεδομένων που συλλέξαμε.

6.2 Honeypots μεσαίας αλληλεπίδρασης

6.2.1 Kippo

Το Kippo είναι μια μεσαία αλληλεπίδραση SSH honeypot γραμμένο σε Python. Το Kippo χρησιμοποιείται για την καταγραφή βίαιων επιθέσεων δυνάμεων και για ολόκληρη την αλληλεπίδραση κελύφους που εκτελείται από έναν εισβολέα. Είναι εμπνευσμένο από τον Kojoney. Ο πηγαίος κώδικας απελευθερώνεται με τη Νέα Άδεια BSD . Το Kippo δεν είναι πλέον σε ενεργό ανάπτυξη και συνιστά τη χρήση του έργου fork'd Cowrie. Παρακάτω αναφέρουμε κάποια ενδιαφέροντα χαρακτηριστικά του όπως και τις απαιτήσεις που έχει ως προς το λογισμικό.

Χαρακτηριστικά:

- Ψεύτικο σύστημα αρχείων με δυνατότητα προσθήκης / κατάργησης αρχείων. Εμφανίζεται ένα πλήρες πλαστό σύστημα αρχείων που μοιάζει με εγκατάσταση του Debian 5.0
- Δυνατότητα προσθήκης ψεύτικων περιεχομένων αρχείων έτσι ώστε ο εισβολέας να μπορεί να "κατεβάσει" αρχεία όπως / etc / passwd. Περιλαμβάνονται μόνο τα ελάχιστα περιεχόμενα του αρχείου
- Αρχεία καταγραφής αποθηκευμένα σε μορφή UML Συμβατό για εύκολη επανάληψη με αρχικούς χρονοδιακόπτες
- Ακριβώς όπως Kojoney, Kippo αποθηκεύει τα αρχεία που έχουν ληφθεί με το wget για μεταγενέστερη επιθεώρηση
- Απάτη, ο ssh προσποιείται να συνδεθεί κάπου, η έξοδος δεν βγαίνει πραγματικά, κλπ

Απαιτήσεις:

- Ένα λειτουργικό σύστημα (δοκιμασμένο σε Debian, CentOS, FreeBSD και Windows 7)
- Python 2.5+
- Twisted 8.0 έως 15.1.0
- PyCrypto
- Zope Interface

6.2.2 Deception Toolkit

Το Deception Toolkit δημιουργήθηκε από τον Fred Cohen το 1998 και είναι από τα πρώτα honeypots. Το DTK είναι ικανό να προσομοιώνει μια ευρεία ποικιλία υπηρεσιών σε ένα σύστημα, και είναι ικανό να αποκρυπτογραφεί πολλούς διαφορετικούς οικοδεσπότες χωρίς να γίνεται αντιληπτό από τους εισβολείς. Ενώ έχει μεγάλες δυνατότητες δεν μπορεί να ενταχθεί σε honeypot υψηλής αλληλεπίδρασης γιατί δεν προσομοιώνει πραγματικό λειτουργικό σύστημα για να αλληλεπιδρά με τον επιτιθέμενο. Επίσης το TDK αποτελείται από μία συλλογή από Perl scripts και C προγράμματα που είναι σχεδιασμένα για λειτουργικά Unix έτσι ώστε να μιμούνται γνωστά τρωτά σημεία. Τέλος το Deception Toolkit είναι ανοικτού κώδικα λογισμικό που από την μία πλευρά είναι καλό γιατί διανέμεται και δωρεάν από την άλλη όμως είναι κακό γιατί μπορεί να αξιοποιηθεί δυνητικά από τον εισβολέα.

6.2.3 Mwcollectd

Το Mwcollectd είναι ένα Honeypot ανοιχτού κώδικα το οποίο θεωρείται το πρώτο γι’ αυτή την κατηγορία. Ο Georg Wicherski είναι αυτός που το ανέπτυξε το 2005.Στη συνέχεια στο τέλος του ίδιου χρόνου κυκλοφόρησε η επόμενη έκδοση 3.0 στην οποία το Mwcollectd ήταν σαφώς βελτιωμένο σε σχέση με το πρώτο. Το 2009 κυκλοφόρησε η τελευταία έκδοση, v4.

Η ενσωμάτωση σε αυτό, των ενοτήτων Python, (modules), λόγο του ότι αυτό έχει γραφτεί σε C++ καθιστούν το Honeypot ευέλικτο και επεκτάσιμο με νέα πρωτόκολλα και χαρακτηριστικά.

Το Mwcollectd και το Nepenthes τα οποία λειτουργούσαν, και τα δυο, με άδεια GNU, στις αρχές του 2006 συγχωνεύτηκαν έχοντας ως αποτέλεσμα, μεγαλύτερη ανάπτυξη και ευρύτερη αποδοτικότητα. Από τότε το νέο Honeypot κυκλοφορεί με την ονομασία Nepenthes διότι ως νέος κώδικας χρησιμοποιήθηκε ο κώδικας Nepenthes λόγο του ότι περιείχε περισσότερα modules. Το νέο Honeypot είναι χαμηλής αλληλεπίδρασης.

6.2.4 Multipot

Το Multipot είναι ένα honeypot εξομοίωσης των Windows το οποίο έχει σχεδιαστεί για να συλλέγει με ασφάλεια τον κακόβουλο κώδικα που διαδίδεται μέσω Backcounts του Malcode και των Windows Exploits. Αρχικά κυκλοφόρησε το 2005 από την iDefence.

6.2.5 HoneySpider

Οι εταιρείες Nask/CERT POLSKA και GOVCERT. NL και Surfnet , δημιούργησαν κοινοπραξία, αναπτύσσοντας το δίκτυο HoneySpider. Η κοινοπραξία, χρησιμοποιώντας τα πλέον προηγμένα Client Honeypots, έθεσαν ως σκοπό τους την ανάπτυξη ενός νέου συστήματος Client Honeypot, το οποίο θα είχε τη δυνατότητα ανίχνευσης διευθύνσεων κακόβουλου περιεχομένου. Αυτό θα μπορούσε να γίνει πράξη στηριζόμενο στη δυνατότητα επεξεργασίας διευθύνσεων URL.

Οι επιθέσεις με τις οποίες αυτό το σύστημα ‘’ασχολείται’’ αφορούν σε Web browsers. Αυτές οι επιθέσεις περιλαμβάνουν: δυαδικά αρχεία κακόβουλου περιεχομένου, απόπειρες ηλεκτρονικού ‘’ψαρέματος’’ ή ανιχνεύσεις ελεγχόμενων διαδικτυακών λήψεων. Ταυτόχρονα το σύστημα αναλύει το κακόβουλο λογισμικό και αναπαράγει μια υπογραφή γι’ αυτό, ψηφιακής μορφής.

Η ουσιαστική αύξηση των επιθέσεων σε browsers, δημιούργησε το κίνητρο ανάπτυξης του δικτύου. Τα υφιστάμενα συστήματα παρακολούθησης, περιλαμβάνουν στην εμβέλειά τους αυτές τις επιθέσεις . Έγινε αναγκαίο όμως να επεκταθούν αυτές οι δυνατότητες παρακολούθησης καθώς και η πρόληψη ενάντια σε απειλές από κακόβουλο λογισμικό. Αναμένεται η σταδιακή βελτίωση του συστήματος στο επίπεδο της επίγνωσης εκ μέρους του χρήστη της εκάστοτε κατάστασης, αλλά και τις προσφερόμενες υπηρεσίες ασφαλείας.

6.2.6 Trigona

Το Trigona Honeypot Σχεδιάστηκε με σκοπό την εξακρίβωση μιας κακόβουλης διεύθυνσης URL. Μια διεύθυνση μπορούμε να την ορίσουμε ως κακόβουλη, βεβαίως εφόσον προσπελαστεί από κάποιο browser, όταν αποκτήσει τη δυνατότητα να εγκαθιστά, στον υπολογιστή του χρήστη, ένα εκτελέσιμο αρχείο.

Επιτρέπει την εκτέλεση ενός προγράμματος στον υπολογιστή, με την προϋπόθεση να μην δεσμεύει άλλους υπολογιστικούς πόρους και να μην επηρεάζει άλλα προγράμματα. Για να πετύχει τα ανωτέρω χρησιμοποιεί την εφαρμογή

Sandboxie, η οποία λειτουργεί σαν ένα sandbox πρόγραμμα. Με τη χρήση του Sandboxie παραμένουν ανοιχτοί, ταυτόχρονα στο ίδιο στιγμιότυπο του Sandboxie πολλαπλοί Internet Explorer Browsers για να προσπελάσουν κακόβουλες URL διευθύνσεις . Στη συνέχεια το Sandboxie μπορεί να εξετάσει το σύστημα αρχείων, κλείνοντάς το, για οποιαδήποτε ύποπτη αλλαγή. Αν οι οποιεσδήποτε αλλαγές ανιχνευτούν και χαρακτηριστούν νέα δυαδικά αρχεία, τότε το περιεχόμενό τους συμπιέζεται και η εκάστοτε διεύθυνση URL, στη βάση των δεδομένων, χαρακτηρίζεται ύποπτη.

Το Trigona Honeypot χρησιμοποιεί τα καλύτερα, χαμηλής και υψηλής αλληλεπίδρασης, Client Honeypots σε συνδυασμό με Perl scripts. Μπορεί να θεωρηθεί ένα Virtual Box το οποίο σχεδιάστηκε για υψηλή απόδοση. Η χρήση υψηλής αλληλεπίδρασης Client Honeypots έχει σαν αποτέλεσμα την καταγραφή αυτών που δεν μπορεί να καταγράψει ένα χαμηλής αντίστοιχης Client Honeypots και αντίστροφα. Όμως τα υψηλής αλληλεπίδρασης είναι πιο αργά σε σχέση με τα χαμηλής τέτοιας, διότι απαιτεί ένα εικονικό μηχάνημα για κάθε διεύθυνση URL που αναλύεται σε αντίθεση με ένα εργαλείο γραμμής εντολών που μπορεί, σε μικρό χρονικό διάστημα, να ελέγξει πολλαπλές συνδέσεις.

6.3 Honeypots υψηλής αλληλεπίδρασης

6.3.1 ManTrap

Το ManTrap είναι ένα εμπορικό honeypot που αναπτύχθηκε, σχεδιάστηκε και πωλείται από την Recourse Technologies. Το ManTrap όχι μόνο μπορεί να χρησιμοποιηθεί για την ανίχνευση επιθέσεων, αλλά μπορεί να χρησιμοποιηθεί για τη συλλογή εκτεταμένων πληροφοριών. Αποτελεί ένα πλήρες λειτουργικό σύστημα που λειτουργεί σαν δόλωμα για τους εισβολείς. Ωστόσο, αυτή η προστιθέμενη λειτουργικότητα και ευελιξία έρχονται με την τιμή της μεγαλύτερης πολυπλοκότητας και κινδύνου.

6.3.2 Capture – HPC

Το Capture είναι ένα honeypot υψηλής αλληλεπίδρασης που αναπτύχθηκε από ερευνητές στο Πανεπιστήμιο Victoria του Wellington, NZ. Η καταγραφή διαφέρει από τους υπάρχοντες honeypots πελατών με διάφορους τρόπους. Πρώτον, έχει σχεδιαστεί για να είναι γρήγορη. Οι κρατικές αλλαγές ανιχνεύονται χρησιμοποιώντας ένα μοντέλο βασισμένο σε συμβάντα που επιτρέπει να αντιδράσει στις μεταβολές της κατάστασης καθώς εμφανίζονται. Δεύτερον, η καταγραφή έχει σχεδιαστεί ώστε να είναι επεκτάσιμη. Ένας κεντρικός διακομιστής Capture είναι σε θέση να ελέγχει πολλούς πελάτες σε ένα δίκτυο. Τρίτον, το Capture υποτίθεται ότι είναι ένα πλαίσιο που επιτρέπει την αξιοποίηση διαφορετικών πελατών. Η αρχική έκδοση του Capture υποστηρίζει τον Internet Explorer, αλλά η τρέχουσα έκδοση υποστηρίζει όλα τα μεγάλα προγράμματα περιήγησης (Internet Explorer, Firefox, Opera, Safari) καθώς και άλλες γνωστές εφαρμογές HTTP, όπως οι εφαρμογές γραφείου και οι συσκευές αναπαραγωγής πολυμέσων.

6.3.3 SHELIA

Το Shelia είναι ένα client honeypot υψηλής αλληλεπίδρασης που αναπτύχθηκε από τον Joan Robert Rocaspana στο Vrije Universiteit Amsterdam. Ενσωματώνεται με έναν αναγνώστη ηλεκτρονικού ταχυδρομείου και επεξεργάζεται κάθε μήνυμα ηλεκτρονικού ταχυδρομείου που λαμβάνει (διευθύνσεις URL & συνημμένα). Ανάλογα με τον τύπο της παραληφθείσας διεύθυνσης URL ή συνημμένου, ανοίγει μια διαφορετική εφαρμογή πελάτη (π.χ. πρόγραμμα περιήγησης, εφαρμογή γραφείου κτλ.) Παρακολουθεί εάν εκτελέσιμες οδηγίες εκτελούνται στην περιοχή δεδομένων της μνήμης (πράγμα που σημαίνει ότι έχει ενεργοποιηθεί μια εκμετάλλευση υπερχείλισης buffer) . Με μια τέτοια προσέγγιση, το SHELIA δεν είναι μόνο σε θέση να ανιχνεύσει τα εκμεταλλεύσιμα, αλλά είναι σε θέση να αποτρέψει πραγματικά τα εκμεταλλεύσιμα από την ενεργοποίηση.

6.3.4 HoneyMonkey

Το HoneyMonkey είναι ένα honeypot υψηλής ευκρίνειας που βασίζεται στο πρόγραμμα περιήγησης (IE) και υλοποιείται από τη Microsoft το 2005. Δεν είναι διαθέσιμο για λήψη. Το HoneyMonkey βασίζεται στο κράτος και εντοπίζει επιθέσεις σε πελάτες παρακολουθώντας αρχεία, μητρώα και διαδικασίες. Ένα μοναδικό χαρακτηριστικό του HoneyMonkey είναι η προσέγγισή του σε πολλά επίπεδα για την αλληλεπίδραση με τους διακομιστές, προκειμένου να εντοπιστούν οι εκμεταλλεύσεις μηδενικής ημέρας. Το HoneyMonkey αρχικά ανιχνεύει τον ιστό με μια ευάλωτη διαμόρφωση. Μόλις εντοπιστεί μια επίθεση, ο διακομιστής επανεξετάζεται με μια πλήρως προσαρμοσμένη διαμόρφωση. Εάν η επίθεση εξακολουθεί να ανιχνεύεται, μπορεί κανείς να συμπεράνει ότι η επίθεση χρησιμοποιεί ένα εκμεταλλευόμενο για το οποίο δεν έχει κυκλοφορήσει ακόμη καμία ενημερωμένη έκδοση και επομένως είναι αρκετά επικίνδυνη.

6.3.5 Web Exploit Finder

Το Web Exploit Finder είναι ένα honeypot το οποίο έχει υλοποιηθεί με τέτοιο τρόπο ώστε να ανιχνεύει επιθέσεις αξιολογώντας τις μεταβολές του λειτουργικού συστήματος. Αναπτύχθηκε από τον Thomas Müller, τον Benjamin Mack και τον Mehmet Arziman, τρεις φοιτητές από το Hochschule der Medien (Stuttgart) 2006. Το WEF μπορεί να χρησιμοποιηθεί ως ένα ενεργό HoneyNet με μια ολοκληρωμένη αρχιτεκτονική εικονικοποίησης κάτω από την οποία μπορούν να μεταφερθούν τα εικονικά μηχανήματα που είναι σε κίνδυνο.

6.3.6 UW Spycrawler

Το UW Spycrawler που αναπτύχθηκε στο Πανεπιστήμιο της Ουάσινγκτον είναι ακόμα ένα client honeypot υψηλής αλληλεπίδρασης που βασίζεται στο Mozilla και αναπτύχθηκε από τους Moshchuk et al. το 2005. Αυτό το honeypot δεν είναι

διαθέσιμο για λήψη. Το UW Spycrawler βασίζεται στα δεδομένα και εντοπίζει επιθέσεις σε πελάτες παρακολουθώντας αρχεία, διαδικασίες, μητρώο και συντριβές προγράμματος περιήγησης. Ο μηχανισμός ανίχνευσης Spycrawlers βασίζεται στο συμβάν. Επιπλέον, αυξάνει το πέρασμα του χρόνου της εικονικής μηχανής που λειτουργεί το Spycrawler για να ξεπεράσει (ή μάλλον να μειώσει την επίδραση) των χρονικών βόμβων.

6.3.7 Google Hack Honeypot

Το Google Hack Honeypot είναι η αντίδραση σε ένα νέο είδος κακόβουλης διαδικτυακής επισκεψιμότητας: χάκερ μηχανών αναζήτησης. Το GHH είναι ένα honeypot "Google Hack". Έχει σχεδιαστεί για να παρέχει αναγνώριση σε επιτιθέμενους που χρησιμοποιούν μηχανές αναζήτησης ως εργαλείο hacking ενάντια στους πόρους σας. Η GHH εφαρμόζει τη θεωρία honeypot για να παρέχει πρόσθετη ασφάλεια στην παρουσία σας στο διαδίκτυο.

Η Google έχει αναπτύξει ένα ισχυρό εργαλείο. Η μηχανή αναζήτησης που έχει εφαρμόσει η Google επιτρέπει την αναζήτηση σε τεράστιο όγκο πληροφοριών. Ο δείκτης Google αυξήθηκε κατά 8 δισ. Σελίδες [Φεβρουάριος 2005] και συνεχίζει να αυξάνεται καθημερινά. Αντικατοπτρίζοντας την ανάπτυξη του δείκτη Google, η διάδοση εφαρμογών που βασίζονται στον ιστό, όπως οι πίνακες μηνυμάτων και τα απομακρυσμένα εργαλεία διαχείρισης, έχει ως αποτέλεσμα την αύξηση του αριθμού των εσφαλμένων και ευάλωτων εφαρμογών ιστού που είναι διαθέσιμες στο Διαδίκτυο.

Αυτά τα μη ασφαλή εργαλεία, σε συνδυασμό με τη δύναμη μιας μηχανής αναζήτησης και ευρετηρίου που παρέχει η Google, οδηγούν σε ένα βολικό διάνυσμα προσβολής για κακόβουλους χρήστες. Το GHH είναι ένα εργαλείο για την καταπολέμηση αυτής της απειλής.

Το GHH τροφοδοτείται από το ευρετήριο μηχανών αναζήτησης Google και τη βάση δεδομένων Google Hacking (GHDB) που διατηρείται από την κοινότητα johnny.ihackstuff.com.

6.3.8 High Interaction Honeypot Analysis Toolkit (HiHAT)

Το εργαλείο ανάλυσης Honeypot υψηλής αλληλεπίδρασης (HIHAT) επιτρέπει τη μετατροπή αυθαίρετων εφαρμογών PHP σε Honeypots υψηλής αλληλεπίδρασης που βασίζονται στο Διαδίκτυο. Επιπλέον παρέχεται ένα γραφικό περιβάλλον χρήστη που υποστηρίζει τη διαδικασία παρακολούθησης του Honeypot και την ανάλυση των αποκτηθέντων δεδομένων.

Μια τυπική χρήση θα μπορούσε να είναι η μετατροπή των PHPNuke, PHPMyAdmin ή OSCommerce σε ένα πλήρως λειτουργικό Honeypot, το οποίο προσφέρει στους χρήστες πλήρη λειτουργικότητα της εφαρμογής, αλλά εκτελεί ολοκληρωμένη καταγραφή και παρακολούθηση στο παρασκήνιο.

Τα χαρακτηριστικά του HIHAT είναι:

- ✓ σαρώνει αυτόματα για γνωστές επιθέσεις.
- ✓ ανιχνεύει SLQ-Injections, (Remote) File Inlcusions, Cross-Site Scripting (XSS), Λήψη απόπειρες λήψης για κακόβουλα αρχεία π.χ. με WGET ή CURL, Εντολές-Ενέσεις κλπ.

- ✓ παρέχει μια λειτουργία επισκόπησης που σας επιτρέπει να αναζητήσετε και να σαρώσετε γρήγορα νέα περιστατικά (ημι-αυτόματη λειτουργία).
- ✓ υποστηρίζει λεπτομερείς πληροφορίες για όλα τα δεδομένα που σχετίζονται με κάθε πρόσβαση στο honeypot. Αυτό περιλαμβάνει αλλά δεν περιορίζεται στα δεδομένα HTTP-GET, HTTP-POST και COOKIE.
- ✓ αποθηκεύει αντίγραφα κακόβουλων εργαλείων σε ασφαλές μέρος για ανάλυση αργότερα.
- ✓ παρέχει μια γεωγραφική, IP-based χαρτογράφηση σχετικά με τις πηγές επίθεσης. Ο δημιουργούμενος χάρτης δείχνει το την προέλευση των επιθέσεων και προσφέρει επιπλέον λεπτομέρειες για κάθε τοποθεσία.
- ✓ δημιουργεί πολυάριθμα στατιστικά στοιχεία σχετικά με το σύνολο της κυκλοφορίας που αναγνωρίζεται στο σύστημα.

6.3.9 HoneyDrive

Το HoneyDrive είναι το κορυφαίο honeypot σε λειτουργικό Linux. Είναι μια εικονική συσκευή (OVA) με εγκατεστημένη την έκδοση Xubuntu Desktop 12.04.4 LTS. Περιέχει πάνω από 10 προεγκατεστημένα και προεπιλεγμένα πακέτα λογισμικού honeypot όπως honeypot Kippo SSH, honeypots malware Dionaea και Amun, honeypot Honeyd χαμηλής αλληλεπίδρασης, honeypot web του Glastopf και Wordpot, κονσέρβα SCADA / ICS honeypot, Thoney και PhoneyC honeyplients . Επιπλέον, περιλαμβάνει πολλά χρήσιμα προκαθορισμένα σενάρια και βοηθητικά προγράμματα για την ανάλυση, απεικόνιση και επεξεργασία των δεδομένων που μπορεί να καταγράψει, όπως Kippo-Graph, Honeyd-Viz, DionaeaFR, στοίβα ELK και πολλά άλλα. Τέλος, στην κατανομή υπάρχουν επίσης περίπου 90 γνωστές αναλύσεις κακόβουλου λογισμικού, ιατροδικαστικά και εργαλεία παρακολούθησης δικτύου.

6.3.10 HonSSH

Το HonSSH είναι ουσιαστικά ένας SSH proxy, ο οποίος ενεργεί σαν επίθεση Man-in-The-Middle. Βρίσκεται ανάμεσα στον εισβολέα και ένα honeypot και υποκινεί τις συνδέσεις SSH. Με αυτόν τον τρόπο μπορεί να καταγράψει όλες τις αλληλεπιδράσεις, τους κωδικούς πρόσβασης εγγραφής (επανεγγραφής) και ακόμη και να καταγράψει αρχεία που κατέβαλε ο εισβολέας στο honeypot για ανάλυση αργότερα.

Τα χαρακτηριστικά του είναι:

- ✓ Καταγράφει όλες τις προσπάθειες σύνδεσης σε αρχείο κειμένου, βάση δεδομένων ή ειδοποιήσεις μέσω ηλεκτρονικού ταχυδρομείου.
- ✓ Όταν ένας εισβολέας στέλνει μια εικασία με κωδικό πρόσβασης, το HonSSH μπορεί να αντικαταστήσει αυτόματα την προσπάθειά του με τον σωστό κωδικό πρόσβασης (επιλογή spoof_login). Αυτό τους επιτρέπει να συνδεθείτε με οποιονδήποτε κωδικό πρόσβασης, αλλά τους συγχέει όταν προσπαθούν να sudo με τον ίδιο κωδικό πρόσβασης.
- ✓ Όλες οι αλληλεπιδράσεις καταγράφονται σε ένα αρχείο καταγραφής TTY (χάρη στο Kippo) το οποίο μπορεί να αναπαραχθεί χρησιμοποιώντας το βοηθητικό πρόγραμμα playlog που περιλαμβάνεται στο Kippo.

- ✓ Μια περίληψη βασισμένη σε κείμενο μιας περιόδου σύνδεσης εισερχομένων καταγράφεται σε ένα αρχείο κειμένου.
- ✓ Οι συνεδρίες μπορούν να προβληθούν ή να καταστρατηγηθούν σε πραγματικό χρόνο (και πάλι χάρη στο Kippo) χρησιμοποιώντας τη διασύνδεση telnet διαχείρισης.
- ✓ Κάνει λήψη ενός αντίγραφου όλων των αρχείων που μεταφέρονται μέσω wget ή scp.
- ✓ Μπορεί να χρησιμοποιήσει το docker για να περιστρέψει νέα honeypots και να τα επαναχρησιμοποιήσει σε ip βάση.
- ✓ Αποθηκεύει όλες τις τροποποιήσεις που έγιναν στο docker χρησιμοποιώντας το σύστημα παρακολούθησης αρχείων.
- ✓ Προηγμένη λειτουργία δικτύωσης για να κοροϊδέψει τις επιτιθέμενες διευθύνσεις IP μεταξύ HonSSH και honeypot.

ΚΕΦΑΛΑΙΟ 7

Σε αυτό το κεφάλαιο θα μιλήσουμε για προηγμένα Honeypots.

7.1 Honeytokens

Στον τομέα της ασφάλειας υπολογιστών, το honeytokens είναι honeypots που δεν είναι συστήματα υπολογιστών. Η αξία τους δεν έγκειται στη χρήση τους, αλλά στην κατάχρηση τους. Ως εκ τούτου, είναι μια γενίκευση τέτοιων ιδεών, όπως οι τιμές honeypot που χρησιμοποιούνται συχνά σε συστήματα προστασίας στοίβας. Τα Honeytokens δεν εμποδίζουν απαραιτήτως οποιαδήποτε παραβίαση των δεδομένων, αλλά δίνουν στον διαχειριστή ένα επιπλέον μέτρο εμπιστοσύνης στην ακεραιότητα των δεδομένων.

Honeytokens είναι πλασματικές λέξεις ή εγγραφές που προστίθενται σε νόμιμες βάσεις δεδομένων. Επιτρέπουν στους διαχειριστές να παρακολουθούν δεδομένα σε καταστάσεις που κανονικά δεν θα μπορούσαν να παρακολουθήσουν, όπως δίκτυα που βασίζονται σε σύννεφο. Εάν τα δεδομένα κλαπούν, οι μάρκες μελιού επιτρέπουν στους διαχειριστές να προσδιορίσουν από ποιον κλέφτηκαν ή πώς διαρρέουν. Εάν υπάρχουν τρεις θέσεις για τα ιατρικά αρχεία, μπορούν να προστεθούν διαφορετικές μάρκες με τη μορφή πλαστών ιατρικών αρχείων σε κάθε θέση. Διαφορετική honeytoken θα ήταν σε κάθε σύνολο εγγραφών.

Εάν έχουν επιλεγεί για να είναι μοναδικά και είναι απίθανο να εμφανίζονται ποτέ στη νόμιμη κυκλοφορία, μπορούν επίσης να ανιχνευθούν μέσω του δικτύου από ένα σύστημα ανίχνευσης εισβολής (IDS), προειδοποιώντας τον διαχειριστή του συστήματος σε πράγματα που διαφορετικά θα παρέμεναν απαρατήρητα. Αυτή είναι μια περίπτωση όπου υπερβαίνουν απλώς τη διασφάλιση της ακεραιότητας και με ορισμένους μηχανισμούς ασφαλείας, μπορεί στην πραγματικότητα να αποτρέψει την κακόβουλη δραστηριότητα, π.χ. με την απομάκρυνση όλων των πακέτων που περιέχουν το honeytoken στο δρομολογητή. Ωστόσο, αυτοί οι μηχανισμοί έχουν παγίδες γιατί θα μπορούσαν να προκαλέσουν σοβαρά προβλήματα εάν το

honeytoken είχε επιλεγεί κακώς και εμφάνισε διαφορετική νόμιμη κίνηση στο δίκτυο, η οποία στη συνέχεια έπεσε.

7.2 Honeynets

Το honeynet είναι ένα ευάλωτο και προσομοιωμένο δίκτυο υπολογιστών που χρησιμοποιεί ένα διακομιστή αποτυχίας που έχει σχεδιαστεί για να ελέγχει την ασφάλεια του δικτύου. Τα Honeynets αναπτύσσονται για να βοηθήσουν τους ειδικούς της ασφάλειας υπολογιστών να βελτιώσουν την ασφάλεια των δικτύων και των συστημάτων. Παρόλο που ενδέχεται να εμφανιστεί σε έναν hacker ως νόμιμο δίκτυο, φιλοξενείται στην πραγματικότητα σε έναν ψεύτικο διακομιστή. Από το σχεδιασμό, τα honeynets δεν επιτρέπονται για αυθεντικές χρήσεις. Εάν υπάρχει πρόσβαση σε ένα honeynet, το μόνο σίγουρο είναι ότι το άτομο που την έχει είναι ένας χάκερ.

7.3 Honeyfarms

Το honeyfarm ή αλλιώς honeypot farm είναι ένα σύνολο από honeypots και σχετικό λογισμικό που είναι μαζεμένο σε μια συγκεκριμένη τοποθεσία. Αυτό βοηθάει στο αντί οι οργανισμοί να εγκαθιστούν μεγάλο αριθμό honeypots ή να τοποθετούν honeypots σε κάθε δίκτυο τους συγκεντρώνουν όλα αυτά που χρειάζονται και τα τοποθετούν σε μία ειδική μονάδα. Το δίκτυο που φτιάχνεται είναι ένας αφιερωμένος πόρος ασφαλείας και ονομάζεται honeypot farm. Άσχετα σε ποιο δίκτυο πραγματοποιούν επίθεση οι εισβολείς ή σε ποιο δίκτυο βρίσκονται την συγκεκριμένη στιγμή όλα ανακατευθύνονται στο honeyfarm. Το honeyfarm μπορεί να μην βρίσκεται καν στον ίδιο χώρο γεωγραφικά με τα δίκτυα παραγωγής. Τέλος η διαχείριση του honeyfarm μπορεί και να μην γίνεται από τον οργανισμό που το χρησιμοποιεί αλλά να το αναθέσει σε ένα τρίτο πρόσωπο ή ακόμα και σε εταιρία.

7.4 FakeAp

Το FakeAp (Fake Access Points) δημιουργήθηκε για να προσελκύει hackers και γενικά εισβολείς με σκοπό να συλλέγει πληροφορίες για αυτούς. Πιο συγκεκριμένα παραπλανεί και ανιχνεύει NetStumblers, Script Kiddies, Wardrivers και άλλους ανεπιθύμητους δημιουργώντας πολλαπλά σημεία πρόσβασης που ακολουθούν το ασύρματο πρωτόκολλο 802.11b. Τέλος το FakeAp διανέμεται ελεύθερα από την GPL και εκτελείται σε λειτουργικά Linux.

7.5 client Honeypots

Τα client Honeypots είναι ενεργές συσκευές ασφαλείας σε αναζήτηση κακόβουλων διακομιστών που προσβάλλουν πελάτες. Το client honeypot παίζει τον ρόλο του πελάτη και αλληλεπιδρά με τον εξυπηρετητή για να εξετάσει εάν έχει σημειωθεί επίθεση. Συχνά η εστίαση των client honeypots είναι στα προγράμματα περιήγησης ιστού, αλλά οποιοσδήποτε πελάτης που αλληλεπιδρά με τους διακομιστές μπορεί να είναι μέρος ενός client honeypot (για παράδειγμα ftp, ssh, email κ.λπ.).

Υπάρχουν διάφοροι όροι που χρησιμοποιούνται για την περιγραφή των client honeypots. Εκτός από το client honeypot, που είναι η γενική ταξινόμηση, ο honeyclient είναι ο άλλος όρος που χρησιμοποιείται γενικά και είναι αποδεκτός. Ωστόσο, υπάρχει μια λεπτότητα εδώ, καθώς ο "honeyclient" είναι στην πραγματικότητα ένα ομόγραφο που θα μπορούσε επίσης να αναφέρεται στην πρώτη γνωστή υλοποίηση client honeypot ανοιχτού κώδικα, αν και αυτό θα πρέπει να είναι σαφές από το πλαίσιο.

Αρχιτεκτονική

Ένα client honeypot αποτελείται από τρία εξαρτήματα. Το πρώτο εξάρτημα, ένα queuer, είναι υπεύθυνο για τη δημιουργία μιας λίστας εξυπηρετητών για την επίσκεψη του πελάτη. Αυτή η λίστα μπορεί να δημιουργηθεί, για παράδειγμα, μέσω της ανίχνευσης. Το δεύτερο στοιχείο είναι ο ίδιος ο πελάτης, ο οποίος είναι σε θέση να κάνει αιτήσεις σε διακομιστές που προσδιορίζονται από το queuer. Μετά την πραγματοποίηση της αλληλεπίδρασης με τον εξυπηρετητή, το τρίτο στοιχείο, μια μηχανή ανάλυσης, είναι υπεύθυνο για τον προσδιορισμό του κατά πόσον έχει σημειωθεί επίθεση στο client honeypot.

Εκτός από αυτά τα εξαρτήματα, τα client honeypots είναι συνήθως εξοπλισμένα με κάποιο είδος στρατηγικής περιορισμού για να αποτρέψουν επιτυχείς επιθέσεις από την εξάπλωση πέρα από το client honeypot. Αυτό επιτυγχάνεται συνήθως με τη χρήση τείχους προστασίας και εικονικών μηχανών.

Ανάλογα με τα παραδοσιακά honeypots διακομιστή, τα client honeypots ταξινομούνται κατά κύριο λόγο από το επίπεδο αλληλεπίδρασης μεταξύ τους: υψηλό ή χαμηλό, το οποίο υποδηλώνει το επίπεδο λειτουργικής αλληλεπίδρασης που μπορεί να χρησιμοποιήσει ο διακομιστής στο client honeypot. Εκτός από αυτό, υπάρχουν επίσης πρόσφατα υβριδικές προσεγγίσεις που υποδηλώνουν τη χρήση τεχνικών ανίχνευσης υψηλής και χαμηλής αλληλεπίδρασης.

7.6 Shadow Honeypots

Το Shadow Honeypots είναι ένα νέο υβριδικής αρχιτεκτονική που συνδυάζει τα καλύτερα χαρακτηριστικά των honeypots και των συστημάτων ανίχνευσης ανωμαλιών. Σε υψηλό επίπεδο, χρησιμοποιούμε μια ποικιλία από ανιχνευτές ανωμαλιών για την παρακολούθηση της κυκλοφορίας σε ένα προστατευμένο δίκτυο ή υπηρεσία.

Η κίνηση που θεωρείται ανώμαλη επεξεργάζεται από το Shadow honeypot για τον προσδιορισμό της ακρίβειας της πρόβλεψης της ανωμαλίας. Το Shadow είναι μια παρουσία του προστατευμένου λογισμικού που μοιράζεται κάθε εσωτερική κατάσταση με μια κανονική ("παραγωγική") παρουσία της εφαρμογή και είναι εξοπλισμένο για την ανίχνευση πιθανών επιθέσεων. Οι επιθέσεις εναντίον του Shadow έχουν πιαστεί και τυχόν αλλαγές απορρίπτονται. Νόμιμη κίνηση που έχει ταξινομηθεί εσφαλμένα θα επικυρωθεί από το Shadow και θα αντιμετωπιστεί σωστά από το σύστημα με διαφάνεια στον τελικό χρήστη. Το αποτέλεσμα της επεξεργασίας μιας αίτησης από το Shadow χρησιμοποιείται για να φιλτράρει τη μελλοντική επίθεση και θα μπορούσε να χρησιμοποιηθεί για την ενημέρωση του ανιχνευτή ανωμαλίας. Η αρχιτεκτονική μας, επιτρέπει στους σχεδιαστές συστημάτων να βελτιώνουν τα συστήματα δεδομένου ότι τα ψευδή θετικά θα φιλτραριστούν από το Shadow.

Δείχνουμε τη σκοπιμότητα της προσέγγισής μας σε μια απόδειξη της εφαρμογής της αρχιτεκτονικής Shadow Honeypot για τον διακομιστή ιστού Apache και το πρόγραμμα περιήγησης Mozilla Firefox. Εμείς δείχνουν ότι παρά τη σημαντική επιβάρυνση του οργάνου μέτρησης του Shadow (έως 20% για τον Apache), ο συνολικός αντίκτυπος στο σύστημα μειώνεται από την
ικανότητα ελαχιστοποίησης του ποσοστού ψευδών - θετικών.

7.7 HoneyPages

Τα honeypages είναι ιστοσελίδες μιας διαδικτυακής εφαρμογής χωρίς καμία πραγματική αξία ή δεδομένα. Δεν υπάρχει κάποιος υπερσύνδεσμος για αυτές τις ιστοσελίδες από τις πραγματικές ιστοσελίδες της εφαρμογής και οι πραγματικοί χρήστες δεν θα μπορούσαν να τις προσπελάσουν. Αντίθετα όμως κάποιος επιτιθέμενος που αναλύει τα αρχεία της διαδικτυακής εφαρμογής, θα έχει μεγάλο συμφέρον για να την προσπελάσει. Επίσης μπορεί να συμβεί το ίδιο αν κάποιος εισβολέας θέλει να βρει όλες τις σελίδες χρησιμοποιώντας εργαλεία αυτόματης σάρωσης της εφαρμογής. Τέλος σε όλες αυτές τις περιπτώσεις τα honeypages καταγράφουν στοιχεία, πληροφορίες και την προέλευσή από τις επισκέψεις που θεωρούνται κακόβουλες.

ΚΕΦΑΛΑΙΟ 8

Σε αυτό το κεφάλαιο θα μιλήσουμε για την αρχιτεκτονική – τοποθέτηση των honeypots. Ουσιαστικά θα περιγράψουμε τη σημασία του honeypot σε κάθε θέση που μπορεί να μπει. Οι θέσεις είναι τρείς και είναι οι εξής:

1. Μπροστά από το τοίχος προστασίας (Internet)
2. Πίσω από το τοίχος προστασίας (Intranet)
3. Στην αποστρατικοποιημένη ζώνη του δικτύου (DMZ)

8.1 Μπροστά από το τοίχος προστασίας (Internet)

Τοποθετώντας το honeypot μπροστά από το τοίχος προστασίας, ο κίνδυνος για τις εσωτερικές εργασίες δεν αυξάνεται. Ένα honeypot θα προσελκύσει και θα παράγει πολλή ανεπιθύμητη κίνηση, όπως port scan ή attack patterns. Τοποθετώντας ένα honeypot έξω από το τείχος προστασίας, τέτοια γεγονότα δεν καταγράφονται από το τείχος προστασίας και ένα εσωτερικό σύστημα IDS δεν θα δημιουργήσει ειδοποιήσεις. Διαφορετικά, θα δημιουργηθούν πολλές ειδοποιήσεις στο τείχος προστασίας ή στο IDS. Πιθανώς το μεγαλύτερο πλεονέκτημα είναι ότι το τείχος προστασίας ή το IDS, καθώς και οποιοιδήποτε άλλοι πόροι, δεν πρέπει να προσαρμοστούν καθώς το honeypot βρίσκεται εκτός του τείχους προστασίας και αντιμετωπίζεται ως οποιοδήποτε άλλο μηχάνημα στο εξωτερικό δίκτυο. Η λειτουργία ενός honeypot δεν αυξάνει συνεπώς τους κινδύνους για το εσωτερικό δίκτυο ούτε εισάγει νέους κινδύνους. Το μειονέκτημα της τοποθέτησης ενός honeypot μπροστά

από το τείχος προστασίας είναι ότι οι εσωτερικοί εισβολείς δεν μπορούν να εντοπιστούν ή να παγιδευτούν τόσο εύκολα. Η τοποθέτηση ενός honeypot μέσα στο DMZ φαίνεται καλή λύση όσο τα άλλα συστήματα μέσα στο DMZ μπορούν να ασφαλιστούν έναντι του honeypot. Τα περισσότερα DMZs δεν είναι πλήρως προσβάσιμα καθώς μόνο οι απαραίτητες υπηρεσίες επιτρέπεται να περάσουν το τείχος προστασίας. Σε μια τέτοια περίπτωση, η τοποθέτηση του honeypot μπροστά από το τείχος προστασίας πρέπει να ευνοείται καθώς το άνοιγμα όλων των αντίστοιχων θυρών της φωτιάς είναι πολύ χρονοβόρο και επικίνδυνο.

8.2 Πίσω από το τοίχος προστασίας (Intranet)

Ένα honeypot πίσω από ένα τείχος προστασίας μπορεί να εισάγει νέους κινδύνους ασφαλείας στο εσωτερικό δίκτυο, ειδικά εάν το εσωτερικό δίκτυο δεν είναι ασφαλισμένο έναντι του honeypot μέσω πρόσθετων τειχών προστασίας. Αυτό θα μπορούσε να είναι ένα ιδιαίτερο πρόβλημα αν τα Ips χρησιμοποιούνται για έλεγχο ταυτότητας. Τοποθετώντας το honeypot πίσω από ένα τείχος προστασίας, είναι αναπόφευκτο να προσαρμόσετε τους κανόνες του τείχους προστασίας εάν επιτρέπεται η πρόσβαση από το διαδίκτυο. Το μεγαλύτερο πρόβλημα προκύπτει μόλις ο εσωτερικός honeypot υποστεί βλάβη από έναν εξωτερικό εισβολέα. Αυτός κερδίζει τη δυνατότητα πρόσβασης στο εσωτερικό δίκτυο μέσω του honeypot. Αυτή η κίνηση θα αχρηστευθεί από το τείχος προστασίας, καθώς θεωρείται ως κίνηση προς το honeypot μόνο, το οποίο με τη σειρά του χορηγείται. Επομένως, η διασφάλιση ενός εσωτερικού honeypot είναι υποχρεωτική, ειδικά αν πρόκειται για ένα honeypot υψηλής συμμετοχής. Ο κύριος λόγος για την τοποθέτηση ενός honeypot πίσω από ένα τείχος προστασίας θα μπορούσε να είναι η ανίχνευση εσωτερικών εισβολέων. Η καλύτερη λύση θα ήταν να τρέξετε ένα honeypot στο δικό του DMZ, επομένως με ένα προκαταρκτικό τείχος προστασίας. Το τείχος προστασίας θα μπορούσε να συνδεθεί απευθείας στο διαδίκτυο ή στο intranet, ανάλογα με το στόχο. Αυτή η προσπάθεια επιτρέπει τον αυστηρό έλεγχο καθώς και ευέλικτο περιβάλλον με μέγιστη ασφάλεια.

ΚΕΦΑΛΑΙΟ 9

Τα honeypots και τα honeynets είναι δημοφιλείς εργαλεία στον τομέα της ασφάλειας δικτύων και της διαδικτυακής εγκληματικότητας. Η ανάπτυξη και η χρήση αυτών των εργαλείων επηρεάζονται από διάφορα τεχνικά και νομικά ζητήματα, τα οποία πρέπει να εξεταστούν προσεκτικά. Σε αυτό το κεφάλαιο, περιγράφουμε τα ζητήματα ιδιωτικής ζωής των honeypots και των honeynet σε σχέση με τις τεχνικές πτυχές τους. Επίσης θα ασχοληθούμε με το νομικό πλαίσιο της ιδιωτικής ζωής και νομικών λόγων για την επεξεργασία δεδομένων. Επιπρόσθετα θα δούμε τη διεύθυνση IP, διότι σύμφωνα με το δίκαιο της ΕΕ θεωρούνται προσωπικά δεδομένα. Η ανάλυση των νομικών θεμάτων βασίζεται στο δίκαιο της ΕΕ και υποστηρίζεται από συζητήσεις σχετικά με την προστασία της ιδιωτικής ζωής και συναφή θέματα.

9.1 Νομικό πλαίσιο προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων στο δίκαιο της ΕΕ

Αυτή η ενότητα παρέχει μια επισκόπηση των σημαντικότερων κανονισμών περί προστασίας της ιδιωτικής ζωής στην ΕΕ που ισχύουν για τα honeypots. Το νομικό πλαίσιο της ΕΕ, που ισχύει για τα honeypots και τα honeynets, αποτελείται από τα ακόλουθα νομικά μέσα:

- Το κύριο ρυθμιστικό μέσο ή το lex generalis του συστήματος προστασίας προσωπικών δεδομένων είναι επί του παρόντος η οδηγία 95/46 / ΕΚ της ΕΕ που εστιάζεται στην προστασία των ατόμων όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και στην ελεύθερη κυκλοφορία των δεδομένων αυτών. Είναι κοινώς γνωστό ως οδηγία της ΕΕ για την προστασία των δεδομένων. Εξασφαλίζει ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, και ιδίως του δικαιώματος στην ιδιωτική ζωή, όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Εξασφαλίζει επίσης την ελεύθερη κυκλοφορία τέτοιων δεδομένων εντός της ΕΕ και ορίζει κανόνες για τη διασυνοριακή ροή δεδομένων εκτός της ΕΕ. Η οδηγία αντικαταστάθηκε από τον κανονισμό 2016/679 της ΕΕ, τον γενικό κανονισμό για την προστασία των δεδομένων (GDPR), ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018. Το GDPR βασίζεται στις ίδιες αρχές με την οδηγία και επομένως δεν θα αλλάξει τους βασικούς χώρους του συστήματος προστασίας των δεδομένων. Ωστόσο, προσθέτει μια σειρά καθηκόντων στον υπεύθυνο επεξεργασίας δεδομένων (το πρόσωπο που επεξεργάζεται τα δεδομένα και καθορίζει το σκοπό της επεξεργασίας) και τα δικαιώματα για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα (ένα αναγνωρίσιμο άτομο, του οποίου τα δεδομένα υποβάλλονται σε επεξεργασία).
- Η οδηγία 2002/58 / ΕΚ της ΕΕ επικεντρώνεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα και στην προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η παρούσα οδηγία είναι κοινώς γνωστή ως οδηγία της ΕΕ για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). Η οδηγία αυτή είναι lex specialis και ρυθμίζει ειδικά την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων όταν πρόκειται για ηλεκτρονικές επικοινωνίες. Πρέπει να χρησιμοποιείται και να ερμηνεύεται σύμφωνα με τη γενική πράξη, η οποία είναι η οδηγία για την προστασία των δεδομένων ή σύντομα το GDPR. Η παρούσα οδηγία καλύπτει και εναρμονίζει ορισμένα ζητήματα ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες. Ορισμένες από αυτές είναι καθολικά δεσμευτικές, π.χ. διατηρώντας την εμπιστευτικότητα της επικοινωνίας και την ειδική ρύθμιση των cookies. Ωστόσο, άλλοι ρυθμίζουν μόνο τις λειτουργίες των παρόχων ηλεκτρονικών επικοινωνιών, π.χ. την αποθήκευση δεδομένων κίνησης και θέσης. Τον Ιανουάριο του 2017, η Ευρωπαϊκή Επιτροπή εισήγαγε μια πρόταση για νέο κανονισμό για την προστασία της ιδιωτικής ζωής. Θα αντικαταστήσει την ισχύουσα οδηγία και, κατά συνέπεια, το υλικό πεδίο εφαρμογής της ενδέχεται να παραμείνει παρόμοιο. Μια από τις ενδιαφέρουσες καινοτομίες είναι μια ρητή έννοια της επικοινωνίας μηχανής με μηχανή που εμπίπτει στο πεδίο εφαρμογής του κανονισμού. Είναι πολύ νωρίς τώρα να εξάγουμε συγκεκριμένα συμπεράσματα, διότι η πρόταση πρέπει να περάσει από το σύνολο της νομοθετικής διαδικασίας.

➢ Το τελευταίο σχετικό νομοθέτημα είναι η οδηγία της ΕΕ για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών (2016/1148 / ΕΕ · οδηγία για τα ΝΑΚ) που τέθηκε σε ισχύ στις 6 Ιουλίου 2016. Ο κύριος σκοπός της οδηγίας ΝΑΚ είναι η εναρμόνιση του κυβερνοχώρου υποδομές ασφαλείας των κρατών μελών, ώστε να μπορούν εύκολα να ανταλλάσσουν πληροφορίες σχετικά με τα περιστατικά ασφάλειας στον κυβερνοχώρο. Ως εκ τούτου, η οδηγία για τα ΝΑΚ μπορεί να χρησιμεύσει ως βάση για την εθνική νομοθεσία, η οποία θα θέσει τα καθήκοντα ανταλλαγής πληροφοριών σε ορισμένους φορείς εκμετάλλευσης honeypot. Ωστόσο, η οδηγία ρητά αναφέρει στο άρθρο. 2 ότι οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με αυτή πρέπει να γίνεται σύμφωνα με νομικές πράξεις για την προστασία των δεδομένων.

9.2 Δεδομένα που συλλέγονται από τα honeypot

Σχεδόν οποιαδήποτε δεδομένα συλλέγονται από τα honeypots μπορεί να θεωρούνται δεδομένα προσωπικού χαρακτήρα. Η πρώτη πτυχή των θεμάτων προστασίας της ιδιωτικής ζωής στα honeypots και τα honeynets είναι ο τύπος των δεδομένων που συλλέγονται. Υπάρχουν δύο γενικές κατηγορίες:

- Το περιεχόμενο των επικοινωνιών
- Πληροφορίες για την καθιέρωση της επικοινωνίας

Ο πρώτος τύπος δεδομένων που συλλέγονται, το περιεχόμενο των επικοινωνιών (δεδομένα περιεχομένου) ρυθμίζεται από την οδηγία της ΕΕ για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες. Σύμφωνα με το άρθρο 2 στοιχείο α) της οδηγίας για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, η επικοινωνία (δεδομένα περιεχομένου) σημαίνει "κάθε πληροφορία που ανταλλάσσεται ή μεταφέρεται μεταξύ πεπερασμένου αριθμού μερών μέσω διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών." Παραδείγματα δεδομένων περιεχομένου είναι τα όργανα τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα περιεχόμενα αρχείων, τα πλήρη πακέτα που έχουν ληφθεί σε ένα τμήμα δικτύου, το ανακατασκευασμένο περιεχόμενο των αλληλεπιδραστικών περιόδων σύνδεσης (π.χ. εντολές που εκτελούνται σε ένα λογαριασμό κελύφους, δακτυλογραφημένοι κωδικοί πρόσβασης κτλ.) Εκτός από το εναρμονισμένο ευρωπαϊκό δίκαιο, νομική ρύθμιση και προστατεύεται από αστικό και ποινικό δίκαιο.

Η έκταση των αρχείων δεδομένων συλλογής περιεχομένου σχετίζεται με το επίπεδο αλληλεπίδρασης του honeypot. Τα honeypots χαμηλής αλληλεπίδρασης συλλαμβάνουν και συλλέγουν μικρότερες ποσότητες αρχείων δεδομένων περιεχομένου από τα μεσαίες αλληλεπιδράσεις και τα υψηλής αλληλεπίδρασης.

Ο δεύτερος τύπος συλλεγμένων αρχείων πληροφοριών είναι οι πληροφορίες για την καθιέρωση της επικοινωνίας (δεδομένα χωρίς περιεχόμενο, δεδομένα συναλλαγών, επίσης γνωστά ως μεταδεδομένα). Πρόκειται κυρίως για δεδομένα κίνησης και θέσης, τα οποία ορίζονται στην οδηγία της ΕΕ για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες, ως εξής:

1. Δεδομένα κίνησης - τυχόν δεδομένα που υποβάλλονται σε επεξεργασία για τη διαβίβαση μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή για τη χρέωση της (άρθρο 6 της εν λόγω οδηγίας)

2. Δεδομένα δεδομένων τοποθεσίας που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών, υποδεικνύοντας τη γεωγραφική θέση του τερματικού εξοπλισμού ενός χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών (άρθρο 7 της εν λόγω οδηγίας).

3. Παραδείγματα δεδομένων συναλλαγής είναι διευθύνσεις IP, θύρες δικτύου, πρωτόκολλα δικτύου, ονόματα λογαριασμών, πληροφορίες κεφαλίδας email, ώρα, ημερομηνία, διευθύνσεις URL ιστότοπων κλπ.

Οι κατηγορίες δεδομένων συναλλαγής που διατηρούνται στα honeypots περιλαμβάνουν:

1. Δεδομένα απαραίτητα για την ανίχνευση και αναγνώριση της πηγής και του προορισμού μιας επικοινωνίας, για παράδειγμα τη διεύθυνση IP και το όνομα τομέα

2. Δεδομένα απαραίτητα για τον προσδιορισμό της ημερομηνίας, της ώρας και της διάρκειας μιας επικοινωνίας (π.χ., χρονική σήμανση)

3. Δεδομένα απαραίτητα για τον προσδιορισμό του τύπου επικοινωνίας, για παράδειγμα πρωτόκολλο Internet (π.χ. ftp, ssh, samba)

4. Δεδομένα απαραίτητα για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών ή για το τι προορίζεται να είναι ο εξοπλισμός τους, για παράδειγμα το λειτουργικό σύστημα

Από την άποψη των honeypots, η διεύθυνση IP, η χρονική σήμανση και το πρωτόκολλο Internet συλλέγονται σε όλα τα honeypots. Λόγω του προαναφερθέντος ευρέος ορισμού των προσωπικών δεδομένων, όλα αυτά πρέπει να θεωρούνται δεδομένα προσωπικού χαρακτήρα που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας για την προστασία των δεδομένων.

9.3 Νομικά θέματα για την επεξεργασία δεδομένων

Οι διευθύνσεις IP που συλλέγονται κατά τη λειτουργία των honeypots και των honeynet μπορούν να είναι δεδομένα προσωπικού χαρακτήρα είτε από τους πελάτες του χειριστή είτε από τρίτους, των οποίων οι συσκευές χρησιμοποιούνται για την επίθεση. Οι πελάτες μπορούν να παράσχουν τη συγκατάθεσή τους για την επεξεργασία των προσωπικών δεδομένων, αλλά αυτό δεν ισχύει για τα τρίτα πρόσωπα. Επιπλέον, συνιστάται να βασιστεί κανείς σε διαφορετικό νομικό λόγο για

τη μεταποίηση παρά στη συγκατάθεση, όταν είναι διαθέσιμη και εφαρμόσιμη. Ο νομικός λόγος πρέπει να επιλέγεται ανάλογα με το σκοπό της επεξεργασίας.

Τα ακόλουθα μπορούν να θεωρηθούν ως σχετικός σκοπός της επεξεργασίας δεδομένων προσωπικού χαρακτήρα εντός των honeypots και των μεμβρανών:

- Για τα honeypots παραγωγής - διασφαλίζοντας την ασφάλεια της υπηρεσίας
- Για ερευνητικά honeypots - έρευνα και πρόληψη μελλοντικών απειλών

Στην πρώτη περίπτωση, ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να βασιστεί στο νόμιμο συμφέρον τους για την ασφάλεια του κυβερνοχώρου του δικτύου του. Η πιθανή βλάβη της ιδιωτικής ζωής για το υποκείμενο των δεδομένων (εκείνων των οποίων οι διευθύνσεις IP υποβάλλονται σε επεξεργασία) είναι πολύ μικρή. Ως εκ τούτου, μπορούν να επεξεργάζονται τα προσωπικά δεδομένα σύμφωνα με το άρθρο. 7 στοιχείο στ) της οδηγίας για την προστασία των δεδομένων. Επιπλέον, η επεξεργασία αυτή είναι επίσης σύμφωνη με το νόμιμο συμφέρον των ιδιοκτητών των οποίων οι συσκευές χρησιμοποιήθηκαν για την επίθεση, δεδομένου ότι η επεξεργασία αυτή θα μπορούσε να βοηθήσει στην επίλυση της ατυχούς κατάστασής τους.

Στη δεύτερη περίπτωση, η κατάσταση είναι πιο περίπλοκη. Το έννομο συμφέρον του υπεύθυνου επεξεργασίας μπορεί να είναι η προώθηση της ασφάλειας στον κυβερνοχώρο και το δικαίωμα να διεκπεραιώνεται σωστά η επιχείρησή του. Αυτά τα συμφέροντα πρέπει να είναι ανάλογα με το δικαίωμα των προσώπων στα οποία αναφέρονται τα δεδομένα για την προστασία της ιδιωτικής ζωής, υπό το πρίσμα της πιθανής βλάβης που προκαλείται από τη μεταποίηση. Δεδομένου ότι η πιθανή βλάβη είναι πολύ χαμηλή, είμαστε πεπεισμένοι ότι ο νομικός λόγος για τη μεταποίηση που θεσπίστηκε στο άρθρο. Το άρθρο 7 στοιχείο στ) θα πρέπει να ισχύει και στην περίπτωση των ερευνητικών honeypots.

Επιπλέον, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να εξετάσει επαρκή χρονική περίοδο για τη διατήρηση των συλλεγόμενων δεδομένων. Και πάλι, συνδέεται με το σκοπό της επεξεργασίας. Όπως αναφέρθηκε προηγουμένως, ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να κατέχει τα δεδομένα μόνο για μια απαραίτητη περίοδο.

Στην περίπτωση των honeypots παραγωγής, τα δεδομένα θα πρέπει να διαγράφονται περιοδικά μετά από μικρότερο χρονικό διάστημα (π.χ. ένα μήνα) ή μόλις επιλυθεί το περιστατικό ασφάλειας. Στην περίπτωση των ερευνητικών honeypots, θα μπορούσε να είναι μεγαλύτερος χρόνος, αλλά δεν πρέπει να υπερβαίνει την αναλογικότητα της Τέχνης. 7 γράμμα στ) νομικό υπόβαθρο. Εάν ο ελεγκτής δεδομένων επιθυμεί να διατηρήσει τα δεδομένα περισσότερο, θα πρέπει να λάβει συναίνεση από τα υποκείμενα των δεδομένων.

Τέλος, ανεξάρτητα από το αν πρόκειται για παραγωγικό ή ερευνητικό honeypot, ο φορέας εκμετάλλευσης honeypot ενδέχεται να έχει νόμιμο καθήκον να ανταλλάσσει πληροφορίες σχετικά με περιστατικά που αφορούν την ασφάλεια του κυβερνοχώρου, όπως για παράδειγμα η οδηγία για τα NAK. Σε τέτοιες περιπτώσεις, τα δεδομένα μπορούν να υποστούν επεξεργασία (και να μεταφερθούν) σύμφωνα με την πρόνοια του άρθρου. 7 στοιχείο γ), όπως προαναφέρθηκε.

Σε περιπτώσεις όπου η μεταφορά δεδομένων δεν προβλέπεται από το νόμο, είναι απαραίτητο να βασίζονται σε διαφορετικές διατάξεις. Σε περίπτωση μεταφοράς δεδομένων εντός των συνόρων της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών και των χωρών με επαρκές επίπεδο προστασίας, θα ήταν και πάλι η Τέχνη. 7 γράμμα στ) νομικό υπόβαθρο. Το άρθρο 25 της οδηγίας για την προστασία των δεδομένων επιτρέπει στην Επιτροπή να δημοσιεύει απόφαση επάρκειας, η οποία αναφέρει ότι η εν λόγω χώρα διαθέτει επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που είναι επαρκές με εκείνο της ΕΕ. Υποστηρίζουμε ότι στην περίπτωση αυτή, το νόμιμο ενδιαφέρον για την επεξεργασία μπορεί να είναι το συμφέρον των χρηστών των δικτύων επικοινωνίας, επειδή η ανταλλαγή πληροφοριών βελτιώνει την ασφάλεια ολόκληρου του οικοσυστήματος του δικτύου. Είναι αλήθεια ότι το ενδιαφέρον αυτό μπορεί να φαίνεται αρκετά αόριστο, αλλά όσο είναι αναλογικό με τα δικαιώματα του υποκειμένου των δεδομένων, είναι νόμιμο. Η αναλογικότητα, από την άποψή μας, διασφαλίζεται από το γεγονός ότι οι διευθύνσεις IP από μόνες τους δεν επιβάλλουν υπερβολική απειλή για την προστασία της ιδιωτικής ζωής. Σε περίπτωση ανταλλαγής πληροφοριών σε εταίρους εγκατεστημένους σε άλλες χώρες, ισχύουν γενικοί κανόνες σχετικά με τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε διασυνοριακό επίπεδο.

ΚΕΦΑΛΑΙΟ 10

Στο πλαίσιο της παρούσας μεταπτυχιακής διατριβής εγκαταστάθηκε και μελετήθηκε ένα SSH honeypot το Kippo. Επιλέχθηκε το Kippo γιατί είναι ένα honeypot μεσαίας αλληλεπίδρασης και σε αντίθεση με τα υψηλής αλληλεπίδρασης δεν απαιτεί σύνθετες υποδομές, οπότε είναι εύκολο να υλοποιηθεί σε οικιακό μηχάνημα.

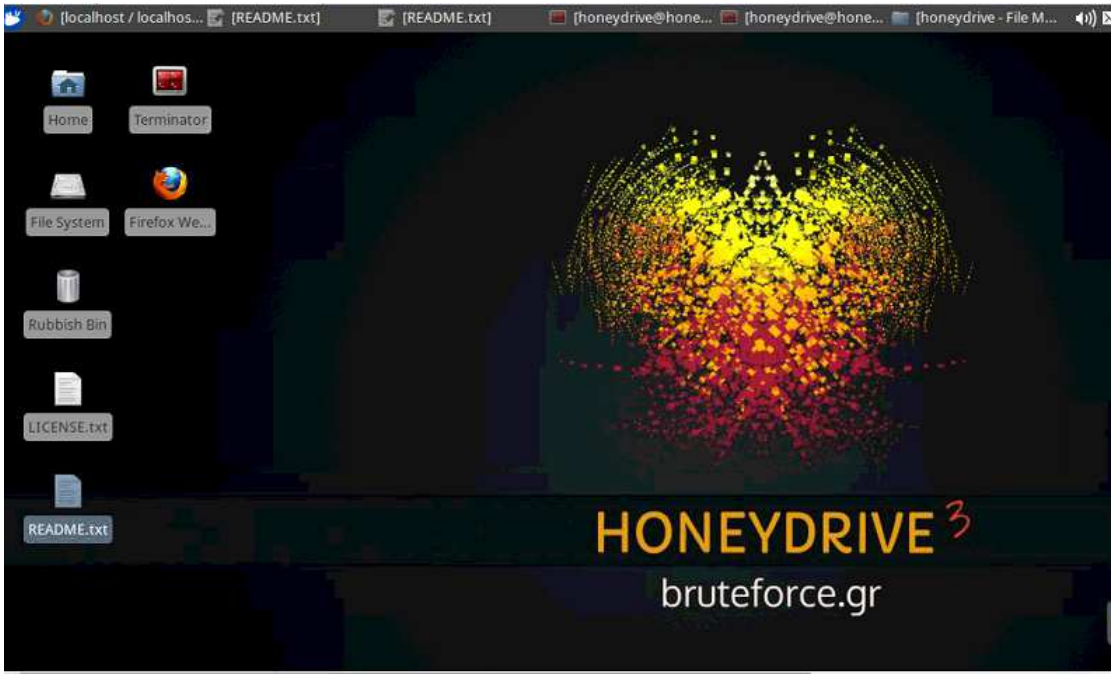
10.1 Περιγραφή πλαισίου υλοποίησης

Για την υλοποίηση του Kippo honeypot χρησιμοποιήθηκε ένας οικιακός υπολογιστής, του οποίου το hardware είναι επεξεργαστής Intel Pentium G3250 3.20GHz, μνήμη ram 6GB και σκληρός δίσκος 500GB. Το λειτουργικό του είναι Windows 7 Professional SP1 64bit στο οποίο έχει γίνει εγκατάσταση του VMware Workstation. Και πάνω στο VMware έκανα εγκατάσταση το honeydrive και του έδωσα δύο πυρήνες, 4GB ram και 80GB δίσκο.

Εικόνα 10.1 : Χαρακτηριστικά του Virtual Machine που φιλοξενεί το HoneyDrive.

10.2 HoneyDrive

Το HoneyDrive είναι μία σουίτα από honeypots με λειτουργικό Xubuntu Desktop 12.04.4 LTS. Η σουίτα αυτή είναι δωρεάν και σε μορφή vmdk (VMware virtual disk file) οπότε είναι εύκολη η εγκατάστασή του στο VMware.



Εικόνα 10.2 : Απεικόνιση της επιφάνειας εργασίας του HoneyDrive.

10.3 Εγκατάσταση του Kippo

Πριν την εγκατάσταση του Kippo είναι απαραίτητο να εγκατασταθούν τα πακέτα python-openssl, python-dev, python-pyasn1, python-mysqldb και openssl. Επίσης χρειάζεται και η εγκατάσταση του phpmyadmin για να μπορούμε να έχουμε πρόσβαση στην βάση δεδομένων του Kippo που είναι MySQL.

Το kippo εξ ορισμού ακούει στη θύρα 2222 όπως αναφέραμε και πιο πάνω όμως λειτουργεί σαν SSH διακομιστής και για να το πετύχουμε αυτό πρέπει να αλλάξουμε την 2222 θύρα του σε 22 και την θύρα του πραγματικού SSH από 22 σε 2222. Με αποτέλεσμα όσοι προσπαθήσουν να επιτεθούν μέσω της θύρας 22 του SSH διακομιστή θα συνδέονται στο Kippo. Αυτό θα το πετύχουμε αλλάζοντάς τη θύρα στο αρχείο των ρυθμίσεων του SSH διακομιστή που βρίσκεται στο κατάλογο /etc/ssh/sshd_config και έπειτα τρέχουμε την εντολή /etc/init.d/ssh restart που κάνει επανεκκίνηση στο διακομιστή.

Επειδή το Kippo για λόγους ασφαλείας δεν μπορεί να εκτελεστεί από τον υπερχρήστη, και τα Linux λειτουργικά από την μεριά τους δεν επιτρέπουν σε κανέναν άλλο χρήστη πλην του υπερχρήστη να χρησιμοποιεί δικτυακές θύρες που είναι κάτω από την 1024 υπάρχει πρόβλημα. Το πρόβλημα αυτό λύνεται με την βοήθεια της εφαρμογής authbind, η εφαρμογή αυτή επιτρέπει σε ένα πρόγραμμα που δεν μπορεί να δουλέψει χωρίς δικαιώματα υπερχρήστη να επικοινωνεί δικτυακά με θύρες οι οποίες απαιτούσαν δικαιώματα υπερχρήστη. Αυτό το πετυχαίνουμε με τις παρακάτω εντολές:

- ✓ Sudo touch /etc/authbind/byport/22
- ✓ Sudo chown kippo:kippo /etc/authbind/byport/22
- ✓ Sudo chmod 777 /etc/authbind/byport/22

Το kippo συλλέγει δεδομένα τα οποία πρέπει κάπου να καταγράφονται και να αποθηκεύονται. Αυτό το επιτυγχάνουμε με μία βάση δεδομένων, οπότε πρέπει να δημιουργήσουμε μία βάση και έναν χρήστη. Παρακάτω ακολουθούν οι εντολές:

mysql –u root –p //σύνδεση στον MySQL διακομιστή
CREATE DATABASE kippo; //δημιουργεί τη βάση kippo
GRANT ALL ON kippo.*TO ‘kippo’@localhost’ IDENTIFIED BY ‘honeydrive’; //δημιουργεί έναν χρήστη kippo στη βάση kippo

mysql –u kippo –p;
USE kippo; //σύνδεση στη βάση kippo με τον χρήστη kippo
source ./doc/sql/mysql.sql; //εισάγει το σχήμα της βάσης που περιέχεται στην έκδοση του kippo

Έπειτα πρέπει να πάμε στο αρχείο kippo.cfg και να αλλάξουμε την θύρα από 2222 σε 22 όπως και να αφαιρέσουμε το σύμβολο # από όλες τις εντολές που είναι υπεύθυνες για την καταγραφή στη βάση δεδομένων για να ενεργοποιηθεί η καταγραφή. Τέλος πρέπει να βάλουμε τον κωδικό του kippo χρήστη στην βάση δεδομένων MySQL.

Μόλις τελειώσουμε όλα τα παραπάνω τα αρχεία του Kippo θα είναι στον κατάλογο /home/kippo και θα είναι τα εξής:

- dl: Εδώ αποθηκεύονται τα αρχεία που λαμβάνουν οι επιτιθέμενοι στο honeypot με την χρήση της εντολής wget.
- log/kippo.log: Αρχείο καταγραφής του kippo.
- log/tty: Εδώ αποθηκεύονται τα αρχεία καταγραφής συνεδριών, με άλλα λόγια οι αλληλεπιδράσεις των επιτιθέμενων με το τερματικό του προγράμματος.
- utils/playlog.py: Script το οποίο μπορεί να αναπαράγει τα αρχεία καταγραφής δεδομένων.
- fs.pickle: Ψεύτικο σύστημα αρχείων του honeypot
- honeyfs: Εδώ βρίσκονται πρόσθετα περιεχόμενα του ψεύτικου συστήματος αρχείων.
- data/userdb.txt: Εδώ βρίσκονται οι πιθανοί συνδυασμοί ονόματος χρήστη και password με τους οποίους κάποιος επιτιθέμενος μπορεί να έχει πρόσβαση στο honeypot.

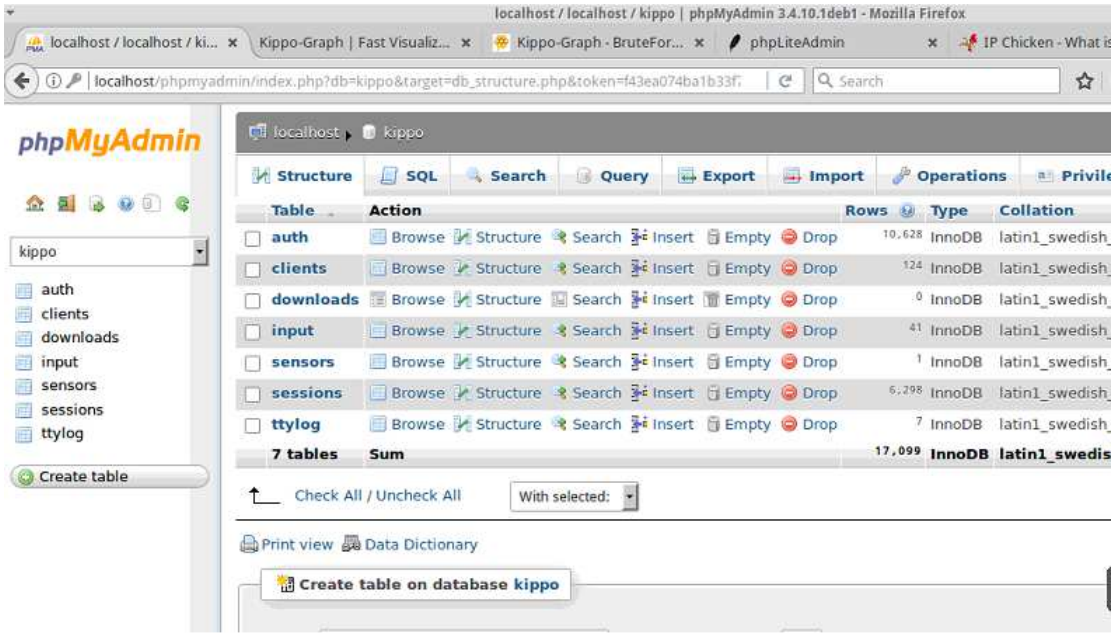
Παρακάτω είναι οι πίνακες της βάσης δεδομένων kippo που δημιουργήσαμε.

- auth: Εδώ καταγράφονται όλες οι προσπάθειες σύνδεσης στον ssh διακομιστή kippo.
- clients: Εδώ καταγράφονται οι διαφορετικοί SSH πελάτες που χρησιμοποιούνται για την σύνδεση στον διακομιστή kippo ssh
- input: Εδώ καταγράφονται οι εντολές που πληκτρολογούνται από τον εισβολέα που έχει εισέλθει στο honeypot.
- sensors: Εδώ αποθηκεύονται τα honeypots που έχουμε δημιουργήσει και στην δική μας περίπτωση το kippo.
- Sesions: Εδώ καταγράφονται όλες οι συνεδρίες που έχουν δημιουργηθεί με τον διακομιστή kippo ssh.
- ttylog: Εδώ καταγράφονται όλα τα δεδομένα του τερματικού honeypot σε δυαδική μορφή.

Για την καλύτερη επισκόπηση της βάσης δεδομένων του kippo πρέπει να εγκαταστήσουμε το εργαλείο phpMyAdmin. Το phpMyAdmin μας βοηθάει στην διαχείριση της εγκατάστασης του MySQL server μέσα από ένα γραφικό περιβάλλον. Αυτό γίνεται με την παρακάτω εντολή:

- ✓ Sudo apt-get install phpmyadmin

Παρακάτω βλέπουμε ένα στιγμιότυπο της βάσης δεδομένων του Kippo από το εργαλείο phpMyAdmin.



Εικόνα 10.3 : Απεικόνιση της βάσης με phpMyAdmin.

Έπειτα από όλα αυτά για να μπορέσει να δουλέψει το honeypot μας πρέπει να απενεργοποιήσουμε το firewall από το router μας και να ανοίξουμε την πόρτα 22. Τέλος τρέχουμε την παρακάτω εντολή από τον κατάλογο του kippo για να ξεκινήσει να λειτουργεί το kippo μας.

10.4 Kippo Graph

Το Kippo-Graph είναι ένα πλήρες σενάριο για την απεικόνιση στατιστικών στοιχείων από ένα honeypot Kippo SSH, αποτελεί λογισμικό ανοικτού κώδικα και είναι διαθέσιμο δωρεάν μέσο της ιστοσελίδας http://bruteforce.gr.

Χρησιμοποιεί τη βιβλιοθήκη σχεδίασης γραφημάτων Libchart PHP από τον Jean-Marc Trémeaux, το QGoogleVisualizationAPI PHP Wrapper για το API οπτικοποίησης Google από τον Thomas Schäfer, τη βιβλιοθήκη RedBeanPHP από την τεχνολογία geolocation Georges de Mooij, MaxMind και geoPlugin.

Το Kippo-Graph παρουσιάζει 24 διαγράμματα, συμπεριλαμβανομένων των 10 κορυφαίων κωδικών πρόσβασης, 10 κορυφαία ονόματα χρηστών, 10 κορυφαίους συνδυασμούς ονόματος χρήστη / κωδικού πρόσβασης, αναλογία επιτυχίας, συνδέσεις ανά IP, συνδέσεις ανά χώρα, ανιχνευτές ημερησίως, καθετήρες ανά εβδομάδα, πελάτες ssh, , κορυφαίες 10 επιτυχείς εισόδους, κορυφαίες 10 αποτυχημένες εισόδους και πολλά άλλα. Υπάρχουν επίσης δεδομένα γεωγραφικής κατανομής που εξάγονται και εμφανίζονται με την τεχνολογία απεικόνισης της Google χρησιμοποιώντας έναν χάρτη Google, έναν χάρτη έντασης κλπ. Τέλος, παρουσιάζονται δεδομένα και στατιστικά στοιχεία που αφορούν την είσοδο, παρέχοντας μια επισκόπηση της δράσης στο εσωτερικό του συστήματος και υπάρχει δυνατότητα αναπαραγωγής συλληφθείσες συνεδρίες

10.5 Εγκατάσταση και ρύθμιση του Kippo Graph

Η εγκατάσταση του Kippo Graph προϋποθέτει την ενσωμάτωση δύο πακέτων λογισμικού στο σύστημα, το οποίο γίνεται με τις εξής εντολές:

apt-get install php5 –gd php5 -mysql
/etc/init.d/apache2 restart
wgethttp://bruteforce.gr/wp-content/uploads/kippo-graph-0.7.2.tar
mv kippo-graph-0.7.2.tar /var/www
cd /var/www
tar xvf kippo-graph-0.7.2.tar –no-same-permissions
cd kippo-graph
chmod 777 generated-graphs

Έπειτα πάμε στο αρχείο config.php και αλλάζουμε τα στοιχεία σύνδεσης με την βάση δεδομένων MySQL όπου βάζουμε τα δικά μας στοιχεία για να μπορεί να συνδέεται στην MySQL του δικού μας kippo.

Τέλος ανοίγουμε κάποιον browzer και πληκτρολογούμε στη γραμμή διευθύνσεων «http://IP διεύθυνση/kippo-graph/» όπου IP διεύθυνση βάζουμε την δικιά μας IP.

10.6 Παρουσίαση δεδομένων του Kippo

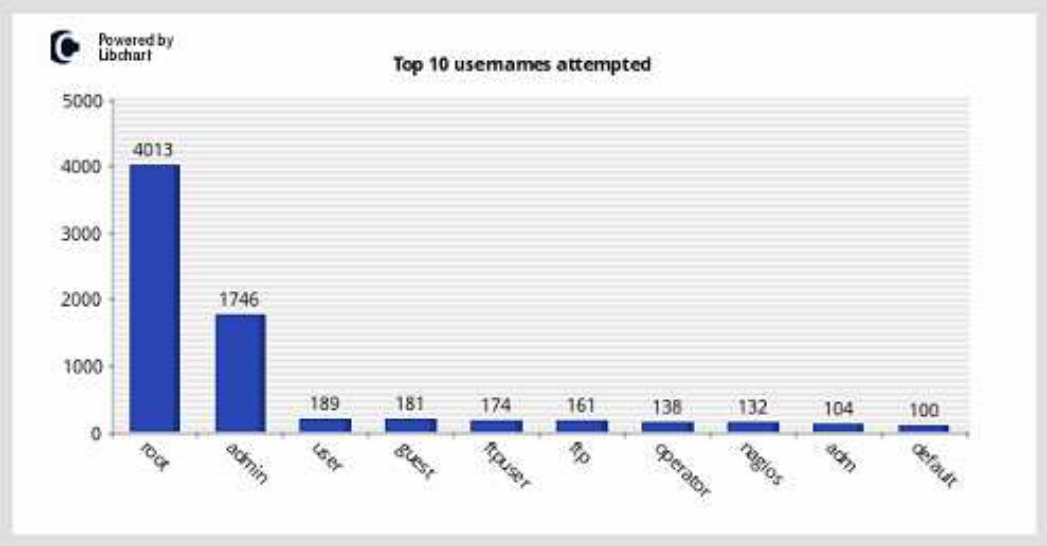
Το Kippo SSH honeypot που παρουσιάσαμε πιο πάνω λειτούργησε για περίπου ένα μήνα και πιο συγκεκριμένα από τις 29 Αυγούστου 2018 έως 19 Σεπτεμβρίου 2018. Το διάστημα αυτό δεν είναι ούτε πολύ μεγάλο άλλα ούτε και πολύ μικρό πιστεύω πώς είναι ικανοποιητικό για την πληρότητα καταγραφής που επιθυμούμε.

Στην περίοδο λειτουργίας του Kippo πραγματοποιήθηκαν συνολικά 10.628 προσπάθειες σύνδεσης, οι οποίες προήλθαν από 124 μοναδικές διευθύνσεις IP. Επίσης κατέγραψε 6.298 συνεδρίες, 41 εντολές από επιτιθέμενους και 7 συνεδρίες σε δυαδική μορφή.

Τα παραπάνω δεδομένα τα πήραμε από την βάση δεδομένων του kippo με την βοήθεια της πλατφόρμας phpMyAdmin.

10.6.1 Ονόματα χρήστη

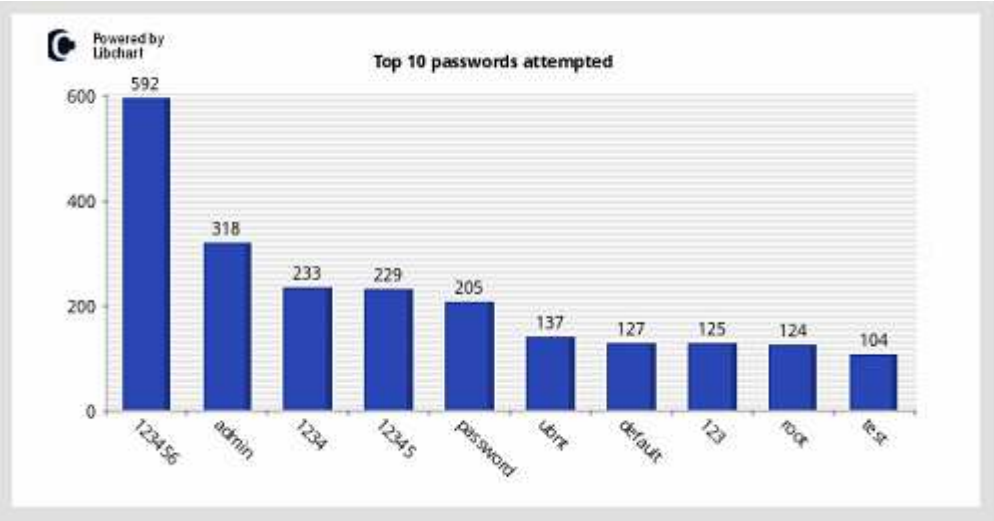
Όπως βλέπουμε και παρακάτω από τα σχεδιαγράμματα που βγάλαμε από το Kippo-Graph παρατηρούμε ότι με συντριπτική πλειοψηφία βγαίνει πρώτο το όνομα χρήστη root με 4013 φορές, έπειτα ακολουθεί το admin με 1746 φορές και τα υπόλοιπα είναι πολύ χαμηλά με κάποιες εκατοντάδες μόνο φορές.



Εικόνα 10.4 : Γράφημα 10 κορυφαίων ονομάτων χρήστη (πηγή Kippo-Graph).

10.6.2 Κωδικοί πρόσβασης (passwords)

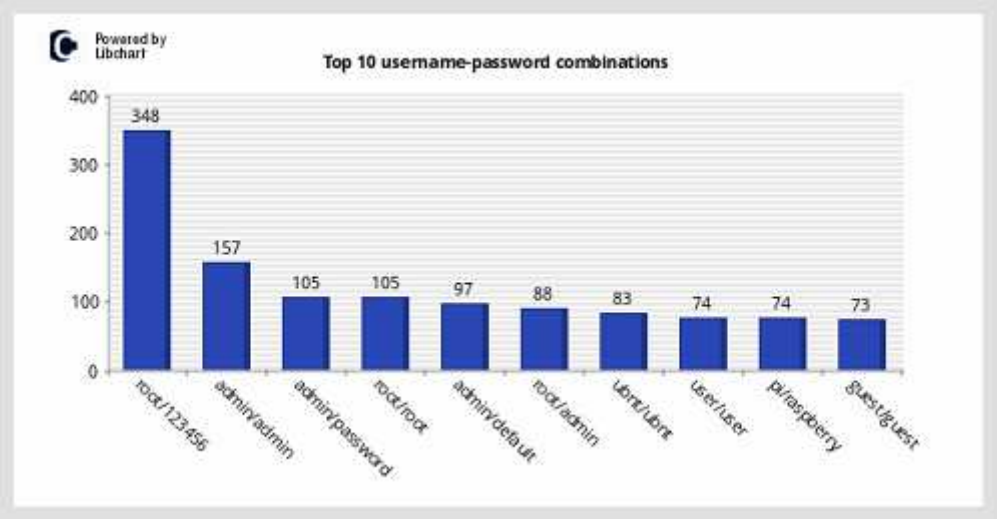
Όσον αφορά τους κωδικούς πρόσβασης που καταγράψαμε παρατηρούμε και εδώ ότι ένας κωδικός είχε συντριπτική πλειοψηφία ο οποίος κωδικός είναι ο 123456. Όπως θα δούμε και παρακάτω στο σχεδιάγραμμα από το Kippo-Graph παρατηρούμε ότι οι επιτιθέμενοι προσπαθούν να συνδεθούν με χρήση συνηθισμένων και απλών passwords.



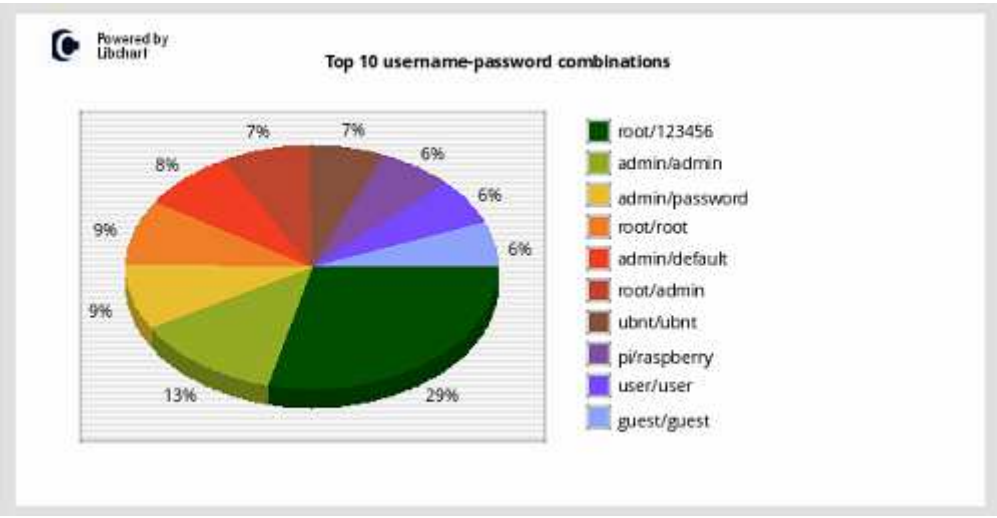
Εικόνα 10.5 : Γράφημα 10 κορυφαίων κωδικών πρόσβασης (πηγή Kippo-Graph).

10.6.3 Συνδυασμός ονόματος χρήστη και κωδικού πρόσβασης

Όπως θα δούμε και παρακάτω στο σχεδιάγραμμα από τις καταγραφές προκύπτει ότι έρχεται πρώτος με μεγάλη διαφορά από τους άλλους συνδυασμούς ο root/123456 με 348 απόπειρες. Αυτό όμως δεν είναι παράξενο ίσα ίσα ήταν και το αναμενόμενο γιατί είναι λογικό οι επιτιθέμενοι να θέλουν να συνδεθούν στο σύστημά μας με δικαιώματα υπερχρήστη.



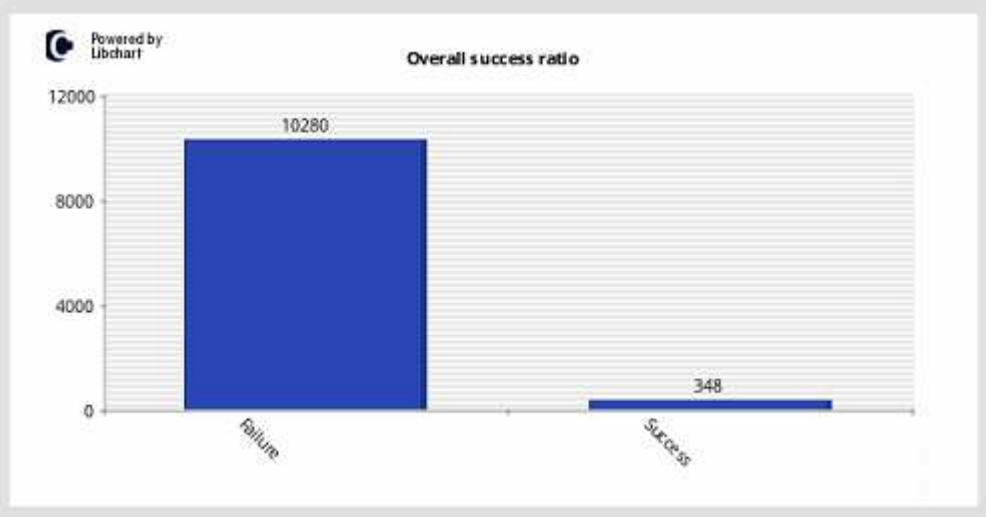
Εικόνα 10.6 : Γράφημα 10 κορυφαίων συνδυασμών ονόματος χρήστη και κωδικού πρόσβασης (πηγή Kippo-Graph).



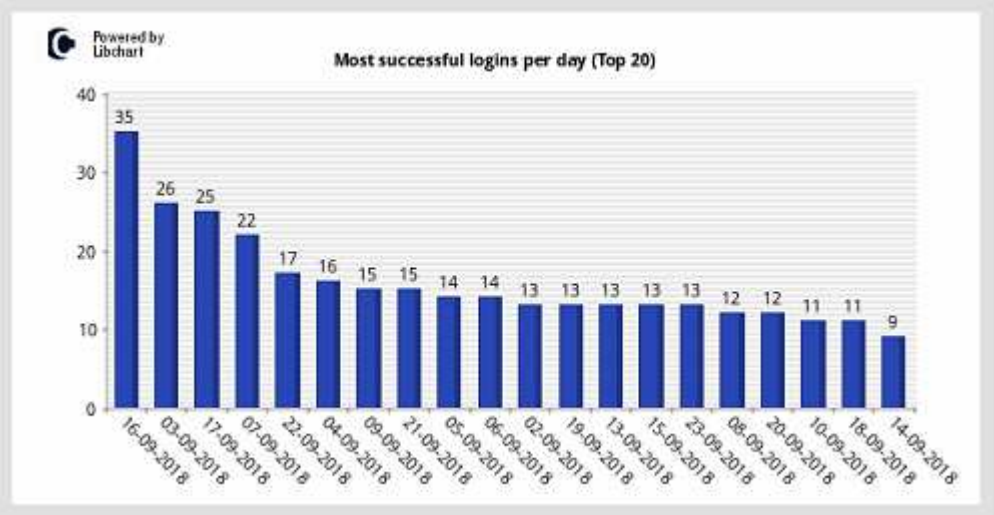
Εικόνα 10.7 : Πίτα 10 κορυφαίων συνδυασμών ονόματος χρήστη και κωδικού πρόσβασης (πηγή Kippo-Graph).

10.6.4 Επιτυχημένες και μη επιτυχημένες προσπάθειες σύνδεσης

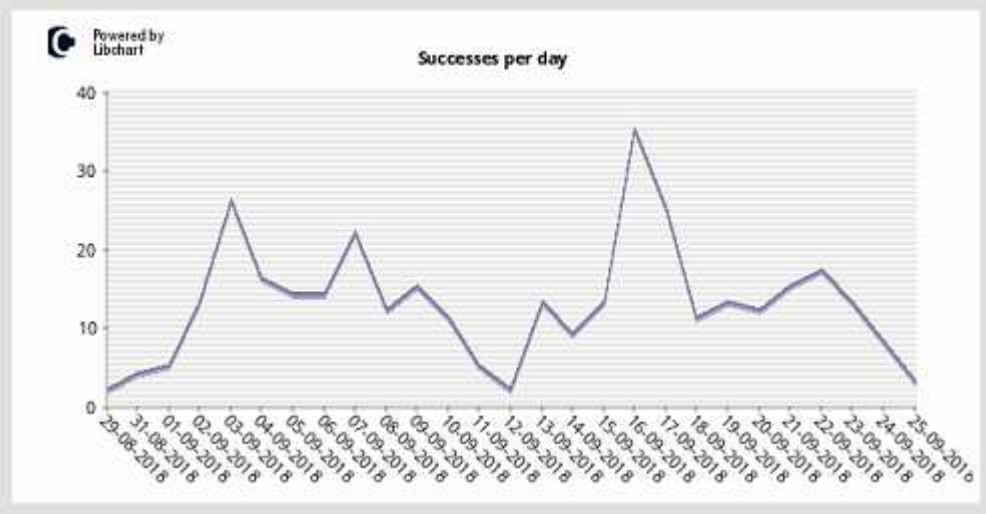
Από ότι θα δούμε παρακάτω στα γραφήματα από το Kippo-Graph παρατηρούμε ότι οι επιτυχημένες προσπάθειες σύνδεσης ήταν ελάχιστες σε σχέση με της ανεπιτυχής αλλά όχι και αμελητέες. Οι επιτυχημένες ήταν 348 έναντι τον μη επιτυχημένων που ήταν 10.280. Επίσης η ημέρα με τις περισσότερες επιτυχημένες προσπάθειες σύνδεσης ήταν η 16 Σεπτεμβρίου 2018 με 35 επιτυχίες και η εβδομάδα με τις περισσότερες επιτυχημένες προσπάθειες ήταν αυτή από τις 5 έως τις 12 Σεπτεμβρίου 2018.



Εικόνα 10.8 : Γράφημα επιτυχημένων και μη επιτυχημένων προσπαθειών σύνδεσης (πηγή Kippo-Graph).



Εικόνα 10.9 : Γράφημα 20 κορυφαίων ημερών με επιτυχημένες συνδέσεις (πηγή Kippo-Graph).

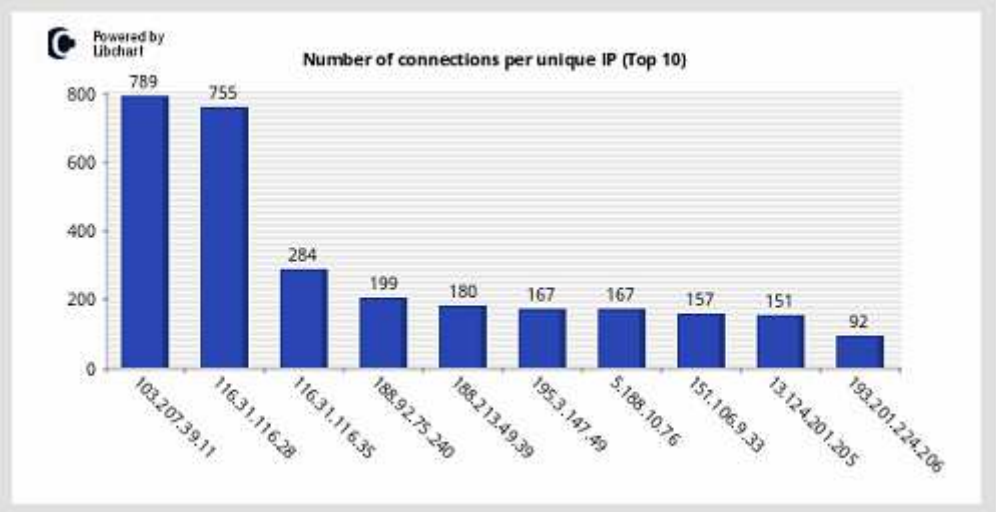


Εικόνα 10.10 : Γράφημα επιτυχημένων προσπαθειών σύνδεσης για τις μέρες λειτουργίας του honeypot (πηγή Kippo-Graph).

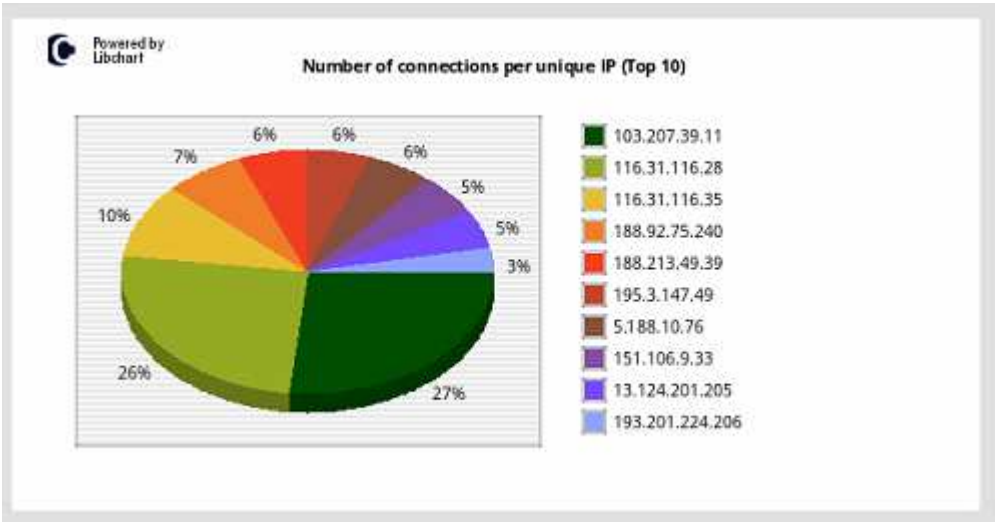
Εικόνα 10.11 : Γράφημα επιτυχημένων προσπαθειών σύνδεσης ανά εβδομάδα για το διάστημα λειτουργίας του honeypot (πηγή Kippo-Graph).

10.6.5 Επιθέσεις με βάση την διεύθυνση IP και την προέλευση

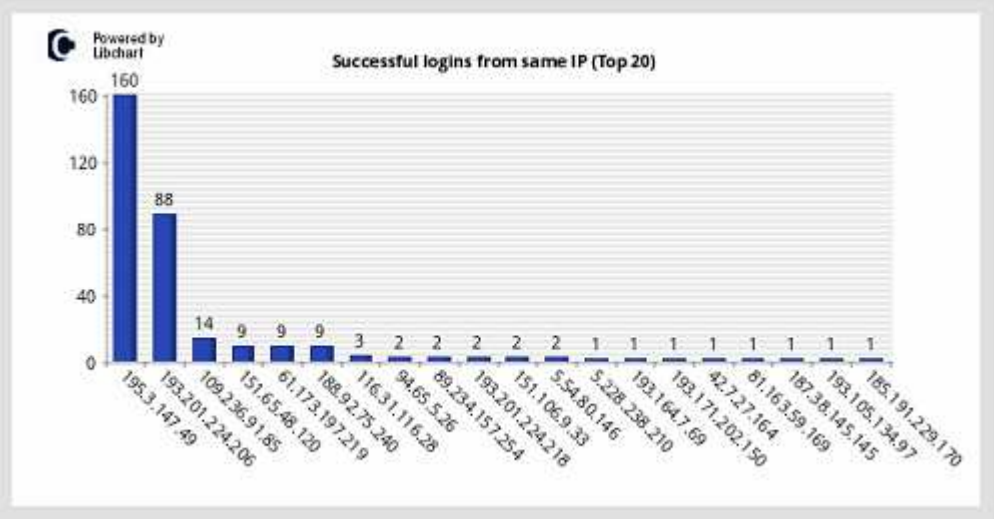
Σύμφωνα με τα παρακάτω γραφήματα παρατηρούμε ότι δύο διευθύνσεις IP κυριάρχησαν με τεράστια διαφορά έναντι των άλλων. Από αυτό όμως δεν μπορούμε να βγάλουμε το συμπέρασμα πως αυτοί οι δύο επιτιθέμενοι ήταν οι πιο επίμονοι όπως δεν μπορούμε και να το αποκλείσουμε κιόλας. Το μόνο που μπορούμε να πούμε είναι πως αυτοί μπορεί να ήταν πιο οργανωμένοι και να είχαν μεγαλύτερα λεξικά για τις επιθέσεις τους.



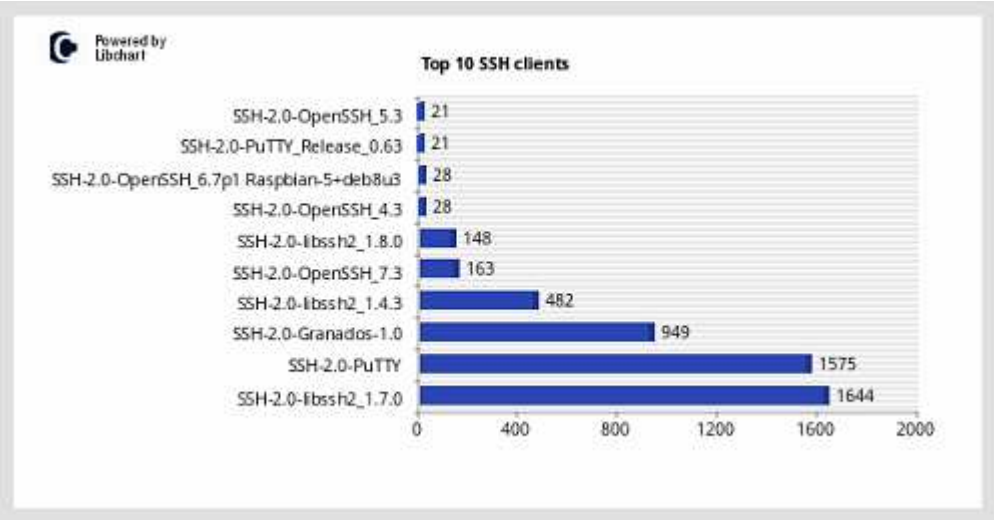
Εικόνα 10.12 : Γράφημα 10 κορυφαίων διευθύνσεων IP με βάση τον αριθμό των επιθέσεων (πηγή Kippo-Graph).



Εικόνα 10.13 : Πίτα 10 κορυφαίων διευθύνσεων IP με βάση το ποσοστό των επιθέσεων (πηγή Kippo-Graph).



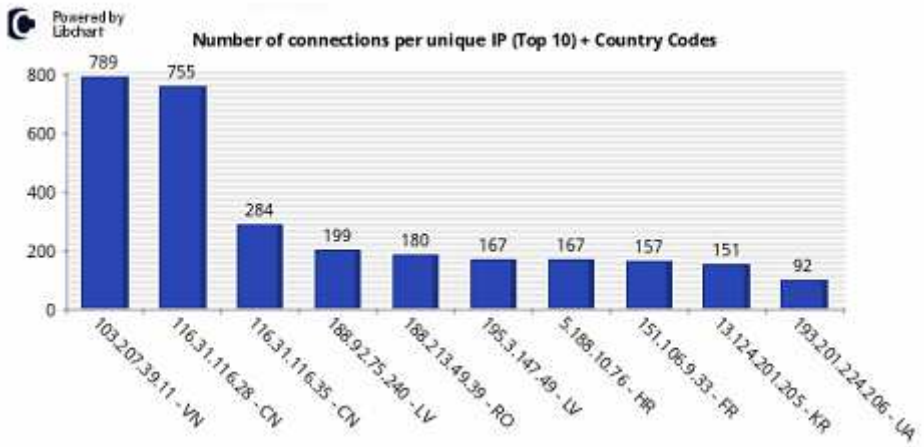
Εικόνα 10.14 : Γράφημα 10 κορυφαίων διευθύνσεων IP με βάση τον αριθμό των επιτυχημένων επιθέσεων (πηγή Kippo-Graph).



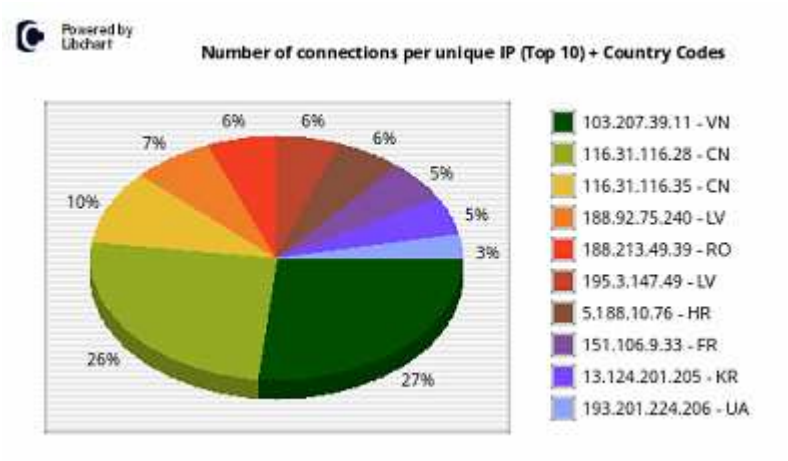
Εικόνα 10.15 : Γράφημα 10 κορυφαίων SSH clients με βάση τον αριθμό των επιθέσεων (πηγή Kippo-Graph).

ID	IP Address	Probes	City	Region	Country Name	Code	Latitude	Longitude	Hostname	Lookup
1	103.207.39.11	789			Vietnam	VN	16	106	103.207.39.11	
2	116.31.116.28	755	Shenzhen	Guangdong	China	CN	22.5333	114.1333	116.31.116.28	
3	116.31.116.35	284	Shenzhen	Guangdong	China	CN	22.5333	114.1333	116.31.116.35	
4	188.92.75.240	199			Latvia	LV	57	25	188.92.75.240	
5	188.213.49.39	180			Romania	RO	46	25	188.213.49.39	
6	195.3.147.49	167			Latvia	LV	57	25	195.3.147.49	
7	5.188.10.76	167	Pula	Istria	Croatia	HR	44.8683	13.8481	5.188.10.76	
8	151.106.9.33	157			France	FR	48.8582	2.3387	151.106.9.33	
9	13.124.201.205	151	Incheon	Incheon	Republic of Korea	KR	37.4536	126.7317	ec2-13-124-201-205.ap-northeast-2.compute.amazonaws.com	
10	193.201.224.206	92			Ukraine	UA	50.45	30.5233	193.201.224.206	

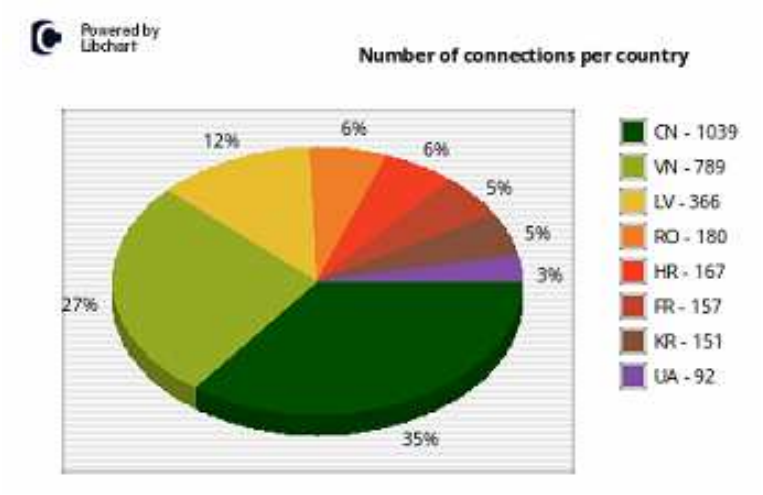
Εικόνα 10.16 : Πίνακας 10 κορυφαίων διευθύνσεων IP με βάση γεωγραφικών και δικτυακών λεπτομερειών (πηγή Kippo-Graph).



Εικόνα 10.17 : Γράφημα 10 κορυφαίων διευθύνσεων IP με βάση τον αριθμό των επιθέσεων, εμφανίζοντας και την χώρα προέλευσης (πηγή Kippo-Graph).



Εικόνα 10.18 : Πίτα 10 κορυφαίων διευθύνσεων IP με βάση τον αριθμό των επιθέσεων, εμφανίζοντας και την χώρα προέλευσης (πηγή Kippo-Graph).



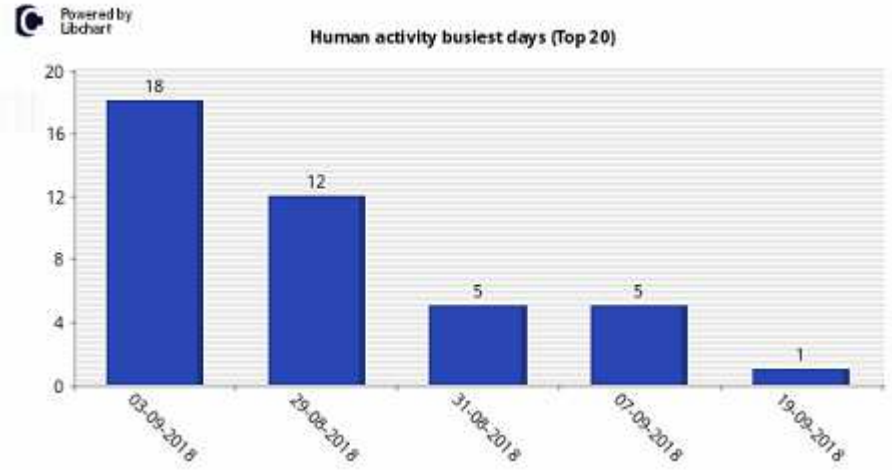
Εικόνα 10.19 : Πίτα 10 κορυφαίων χωρών που προέρχονται οι επιθέσεις με βάση το ποσοστό των επιθέσεων (πηγή Kippo-Graph).

Εικόνα 10.20 : Χάρτης με γεωγραφική κατανομή 10 κορυφαίων διευθύνσεων IP με βάση τον αριθμό των επιθέσεων (πηγή Kippo-Graph).

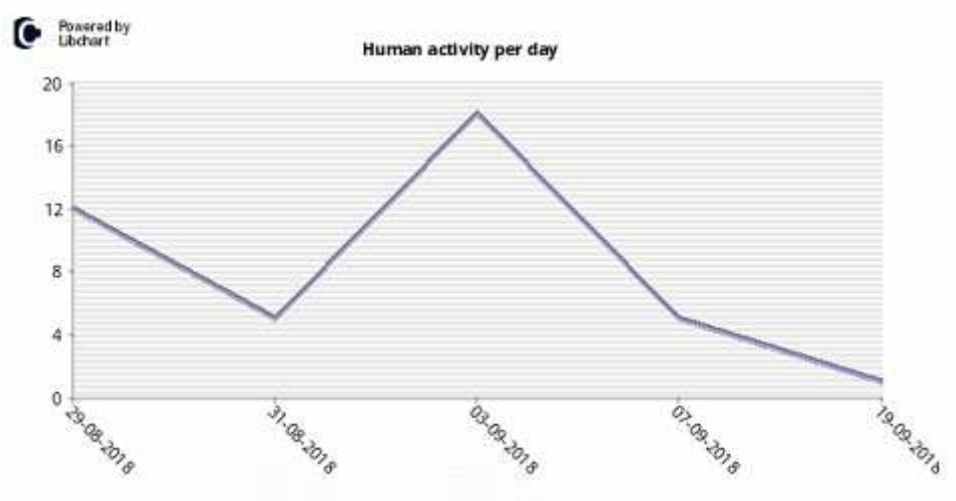
Εικόνα 10.21 : Χάρτης με γεωγραφική κατανομή ανά χώρα των επιθέσεων με προέλευση τις 10 κορυφαίες διευθύνσεις IP (πηγή Kippo-Graph).

10.6.6 Εντολές και ενέργειες που εκτελέστηκαν στο Kippo

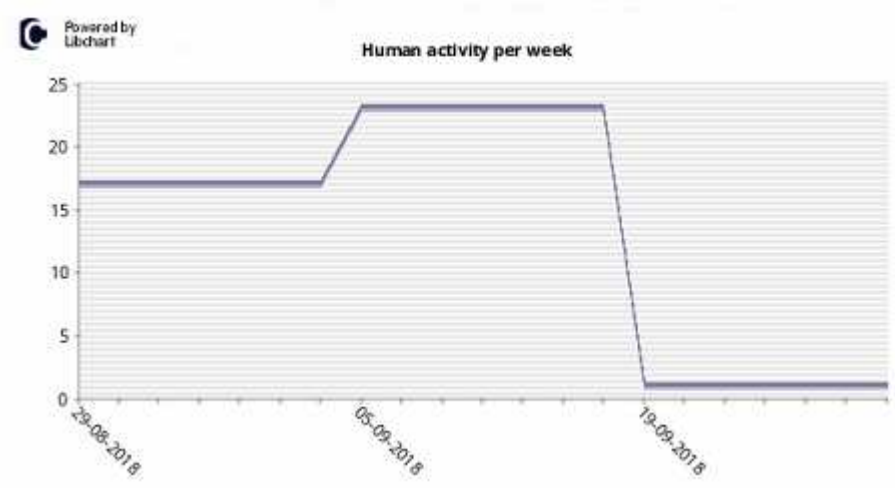
Στο kippo honeypot καταγράφηκαν συνολικά 41 εντολές. Οι πιο πολλές εντολές καταγράφηκαν στις 3 Σεπτεμβρίου 2018 που ήταν 18, ακολουθούν στις 29 Αυγούστου 2018 με 12 έπειτα ισοβαθμούν οι 31 Αυγούστου 2018 και 7 Σεπτεμβρίου 2018 με 5 εντολές και τέλος στις 19 Σεπτεμβρίου 2018 με μόνο μία. Παρακάτω ακολουθούν τα γραφήματα.



Εικόνα 10.22 : Γράφημα 20 κορυφαίων ημερών με βάση την δραστηριότητα εντός του kippo (πηγή Kippo-Graph).

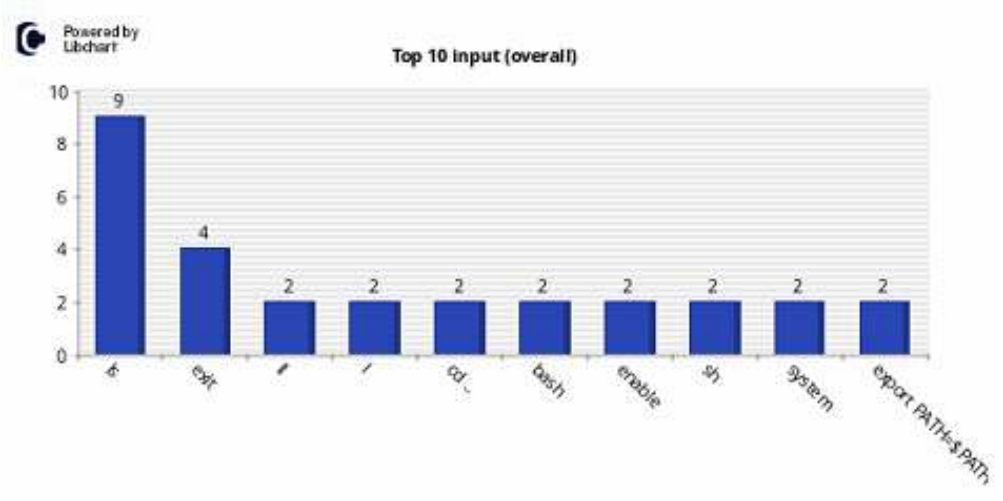


Εικόνα 10.23 : Γράφημα ανθρώπινης δραστηριότητας ανά μέρα (πηγή Kippo-Graph).

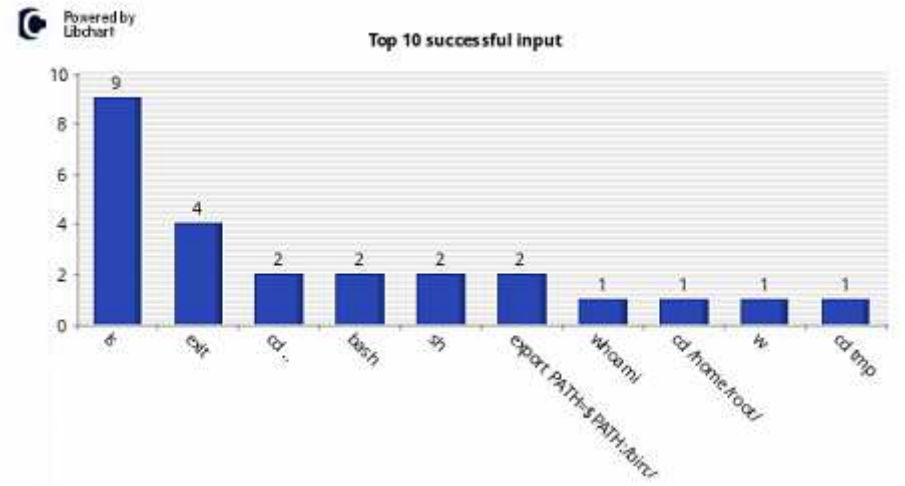


Εικόνα 10.24 : Γράφημα ανθρώπινης δραστηριότητας ανά μέρα (πηγή Kippo-Graph).

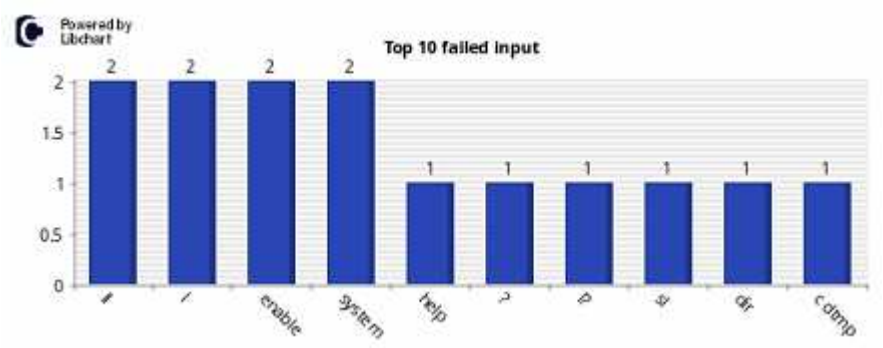
Η εντολή που χρησιμοποιήθηκε πιο συχνά είναι η ls η οποία χρησιμοποιήθηκε 9 φορές και αυτό που κάνει είναι να εμφανίζει τα περιεχόμενα του τρέχοντος καταλόγου. Ακολουθεί η εντολή exit με 4 φορές οι οποία τερματίζει την διεργασία που εκτελείται. Παρακάτω βλέπουμε τις 10 κορυφαίες εντολές που χρησιμοποιήθηκαν και πόσες φορές η κάθε μία σε γράφημα, τις 10 κορυφαίες επιτυχημένες εντολές και τις 10 κορυφαίες μη επιτυχημένες εντολές.



Εικόνα 10.25 : Γράφημα 10 κορυφαίων εντολών που πληκτρολογήθηκαν εντός του kippo με βάση το πλήθος (πηγή Kippo-Graph).



Εικόνα 10.26 : Γράφημα 10 κορυφαίων εντολών που πληκτρολογήθηκαν με επιτυχία εντός του kippo με βάση το πλήθος (πηγή Kippo-Graph).



Εικόνα 10.27 : Γράφημα 10 κορυφαίων εντολών που πληκτρολογήθηκαν χωρίς επιτυχία με βάση το πλήθος (πηγή Kippo-Graph).

10.7 Συμπεράσματα

Στην παρούσα μεταπτυχιακή διατριβή παρουσιάστηκε η έννοια του honeypot ως ένα ερευνητικό εργαλείο που έχει ως σκοπό τη συγκέντρωση πληροφοριών για τη δράση της κοινότητας των κακόβουλων χρηστών, αλλά και ως ένα σύστημα με στόχο την προστασία των συσκευών που βρίσκονται σε ένα δίκτυο από επιθέσεις. Τα honeypots για να καταφέρουν τους εισβολείς να εξαπολύσουν επιθέσεις εναντίον τους λειτουργούν ως συσκευές εξαπάτησης. Με την σειρά τους οι υπεύθυνοι διαχειριστές αφού έχουν συγκεντρώσει τα δεδομένα μπορούν να μελετήσουν τις τεχνικές και τις μεθόδους που χρησιμοποιούν οι επιτιθέμενοι.

Κατά την διάρκεια της διατριβής υλοποιήθηκε το honeypot kippo, μια διαδικτυακή παγίδα για επιτιθέμενους που έχουν ως στόχο την υπηρεσία SSH. Το kippo παρέμεινε σε λειτουργία και συνδεδεμένο με το διαδίκτυο για ένα εύλογο χρονικό διάστημα κατά την διάρκεια του οποίου κατέγραφε επιθέσεις εναντίον του. Από τα στοιχεία που κατέγραψε μπορούμε να συμπεράνουμε ότι η ύπαρξη μίας μόνο ανοιχτής θύρας προσελκύει χιλιάδες εισβολείς και ότι με το να χρησιμοποιούμε εύκολο όνομα χρήστη και κωδικό πρόσβασης επιτρέπουμε στους επιτιθέμενους την εύκολη εισαγωγή στο μηχάνημα και την διενέργεια οποιασδήποτε δραστηριότητας σε αυτό.

10.8 Μελλοντικές Χρήσεις

Εκτός από τον τομέα των δικτυακών επιθέσεων που αναφερθήκαμε και μελετήσαμε σε αυτήν την διπλωματική εργασία, είναι πολύ διαδεδομένος και ο τομέας επιθέσεων σε διαδικτυακές εφαρμογές. Οι επιθέσεις σε αυτές τις εφαρμογές έχουν ως στόχο διαδικτυακές εφαρμογές οι οποίες προσφέρονται δημόσια σε νόμιμους χρήστες. Τέτοιες εφαρμογές είναι φτιαγμένες με διαδικτυακές γλώσσες προγραμματισμού όπως είναι η PHP, η Ruby on Rails, η ASP και άλλες. Πολλοί προγραμματιστές τέτοιων εφαρμογών δεν είναι ενημερωμένοι για τον τρόπο

επίθεσης και τους κινδύνους που υπάρχουν ενάντια στο έργο τους, με αποτέλεσμα να αυξάνονται όλο και πιο πολύ οι επιθέσεις σε διαδικτυακές εφαρμογές με σκοπό την μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα. Για το λόγο αυτό θα έχει πολύ ενδιαφέρον η δημιουργία κάποιου web honeypot που να καταγράφει τέτοιες επιθέσεις.

Στις μέρες μας τα έξυπνα τηλέφωνα (smartphones) είναι πολύ δημοφιλές στους καταναλωτές και θα μπορούσαμε να πούμε πως χρησιμοποιούνται περισσότερο από ότι οι παραδοσιακοί υπολογιστές για την πλοήγηση στο διαδίκτυο. Παράλληλα όμως έχουμε δει ότι δεν παρέχουν μεγάλη ασφάλεια στους χρήστες τους. Και η Apple με το iOS όσο και η Google με το Android έχουν δεχτεί κατά καιρούς επιτυχημένες επιθέσεις που με την σειρά τους τα λειτουργικά τους έγιναν πλατφόρμες εκτέλεσης κακόβουλων ενεργειών προς τους χρήστες τους. Αυτό έγινε είτε μέσω δικτυακών επιθέσεων είτε με την εγκατάσταση κάποιου κακόβουλου λογισμικού. Για το λόγο αυτό τα honeypots θα μπορούσαν να χρησιμοποιηθούν ως ανιχνευτές επιθέσεων σε smartphones καθώς και σαν προσομοιωτές συσκευών για την λήψη κακόβουλου λογισμικού.

ΠΗΓΕΣ

Wikipedia. Δίκτυο υπολογιστών. [online] [cited 23/1/2019] <https://el.wikipedia.org/wikiwiki/Δίκτυο_υπολογιστών>.

Wikipedia. Διαδίκτυο. [online] [cited 20/1/2019] <https://el.wikipedia.org/wiki/Διαδίκτυο>.

Δημήτρης Γκρίτζαλης, ‘’Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση’’ Εκδόσεις Νέων Τεχνολογιών, (pp. 25-26) (2004)

E. Amoroso, Fundamentals of computer security technology. Prentice-Hall, (1994)

J. McCumber, Assessing and Managing Security Risk in IT Systems ‘’A Structured Methodology. Auerbach Publications (2004)

E. Skoudis, Counter Hack ‘’A step by step Guide to Computer Attacks and Effective Defences. Prentice Hall PTR (2002)

R. Moir ‘’Defining Malware: FAQ’’ Microsoft TechNet [online] [cited 10/3/2013] < https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)>

Internet Systems Consortium, ‘’Internet host count history’’ [online] [cited 31/10/2016] < https://www.isc.org/solutions/survey/history>.

Wikipedia. Ασφάλεια πληροφοριακών συστημάτων. [online] <https://el.wikipedia.org/wikiwiki/ Ασφάλεια_πληροφοριακών_συστημάτων>.

L. Spitzner, ‘’Honeypots : Simple, cost-effective detection’’ Security Focus, Infocus 1690, [online] [cited 30/4/2003] < https://www.symantec.com/connect/articles/honeypots-simple-cost-effective-detection>.

NWS and PM, ‘’Anomalie – detection – geraete’’ Network Computing, 2004.

PC Magazine’s Encyclopedia, ‘’definition of Honeypot’’, (2009). [online] [cited 20/12/2012] <http://www.pcmag.com/encyclopedia/term/44335/honeypot>.

Wikipedia. Παγκόσμιος ιστός [online] [cited 17/10/2018] <https://el.wikipedia.org/wiki/Παγκόσμιος_Ιστός> .

Wikipedia. Ιός υπολογιστή [online] [cited 19/2/2019]
< https://el.wikipedia.org/wiki/Ιός_υπολογιστή>.

Wikipedia. Σκουλήκι υπολογιστή [online] [cited 1/2/2019]
< https://el.wikipedia.org/wiki/Σκουλήκι_υπολογιστή>.

Wikipedia. Δούρειος Ίππος (υπολογιστές) [online] [cited 30/12/2018]
< https://el.wikipedia.org/wiki/Δούρειος_Ίππος_(υπολογιστές)>.

Bitdefender. Μάθετε τι είναι το Firewall [online] [cited 17/4/2016]
< https://bitdefender.gr/blog/blog-firewall-advice/>.

E. Peter and T. Schiller, A Practical Guide to Honeypots. USA: Washington University, 2008. [online] [cited 25/12/2012]
< https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/>.

Σ. Τρούλης, Μελέτη Χαμηλής και Υψηλής Αλληλεπίδρασης Honeypots. Πτυχιακή εργασία. Πανεπιστήμιο Πειραιώς, Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων. (Μάιος 2010).

Mokube and M. Adams, ''Honeypots: Concepts, Approaches and challenges'' Proceedings of the 45th annual southeast regional conference, (pp 321-326). (2007)

L. Spitzner, Honeypots : Tracking Hackers. Boston, MA : Addison Wesley, 2003.

C. Stoll, The Cuckoo's Egg. Pocket Books, 1990.

The Honeynet Project, Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Addison Wesley, 2001.

The Honeynet Project ''Know your enemy : Honeynets. What a honeynet is, its value, how it works, and risk/issues involved'' [online] [cited 31/5/2006]
< http://old.honeynet.org/papers/honeynet/>.

The Honeynet Project ''Know your enemy : Genii honeynets. Easier to deploy, harder to detect, safer to maintain'' [online] [cited 12/5/2005]
< http://old.honeynet.org/papers/gen2/>.

The Honeynet Project ''Know your enemy: Sebek'' [online] [cited 17/11/2003]
< http://old.honeynet.org/papers/sebek.pdf>.

N. Provos, Developments of the Honeyd Virtual Honeypot. [online] [cited 5/1/2013]
< http://www.honeyd.org/>.

Freshmeat, Tiny Honeypot, [online] [cited 15/7/2002]
< http://freshmeat.sourceforge.net/projects/thp>.

Nepenthes – Finest Collection. [online] [cited 7/1/2013]
< http://nepenthes.carnivore.it/>.

N. Provos ''A Virtual Honeypot Framework'' 2004.

The Honeynet Project ''Know your enemy: Tracking botnets'' P. Bacher T. Holz et al. [online] [cited 8/10/2008]
< http://www.honeynet.org/papers/bots>.

P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling ''The Nepenthes Platform: An Efficient Approach to Collect Malware'' 2006.

L. Rist ''Know Your Tools: Glastopf'' 2010.

R. Carmo, M. Nassar and O. Festor ''Artemisa: an Open-Source Honeypot Back-End to Support Security in VoIP Domains'' in 12th IFIP/IEEE International Symposium on Integrated Network Management, 2011

H. Bos ''Shelia: A client-side honeypot for attack detection'' [online] [cited 15/12/2012]
< https://www.cs.vu.nl/~herbertb/misc/shelia/>.

I. Koniaris ''HoneyDrive" BruteForce Lab's Blog [online] [cited 10/10/2012]
< https://bruteforcelab.com/honeydrive>.

The Monkey – Spider Project [online] [cited 11/01/2013]
< http://monkeyspider.sourceforge.net/index.html>.

Google Code, kippo – SSH Honeypot [online] [cited 12/1/2013]
< https://github.com/desaster/kippo>

Mark Dargin, '' Increase your network security: Deploy a honeypot'' [online] [cited 24/10/2017]
< https://www.networkworld.com/article/3234692/increase-your-network-security-deploy-a-honeypot.html>.

LaBrea ''Sticky'' honeypot and IDS. [online] [3/2/2013]

< http://labrea.sourceforge.net/labrea-info.html>

J. Gobel, ''Amun: A Python Honeypot'' (2009)

L. Rist ''Know Your Tools: Glastopf'' (2010)

PhoneyC – Python Honeyclient [online] [cited 7/1/2013]
< https://code.google.com/archive/p/phoneyc/>

L. Spitzner ''Honeypot Farms'' [online] [cited 11/8/2003]
< https://www.symantec.com/connect/articles/honeypot-farms>.

Pavol Soko, Jakub Míšek and Martin Husák '' Honeypots and honeynets: issues of privacy'' [online] [cited 28/2/2017]
<https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-017-0057-4>.

S. Vetsch, ''GlastopfNG A Web Attack Honeypot'' (2010)

Kostas G. Anagnostakis, Stelios Sidiroglou,Periklis Akritidis, Michalis Polychronakis, Angelos D. Keromytis, Evangelos P. Markatos '' Shadow Honeypots'' [online] [cited 9/9/2010]
< https://www.ics.forth.gr/_publications/shadow.honeypots.ijcns.pdf>.

Puri. Ramneek ''Bots and botnet: An overview'' Sans Institute (2003).

Australian Honeynet Project, Tool release: Trigona [online] [cited 1/6/2012]
< http://www.honeynet.org.au/?q=node%2F63>

P. Bacher, T. Holz et al. ''Know your enemy: Tracking botnets'' The Honeynet Project. [online] [cited 10/8/2013]
< http://www.honeynet.org/papers/bots>.

H. Bos, ''Shelia: A client – side honeypot for attack detection'' [online] [cited 15/12/2012]
< https://www.cs.vu.nl/~herbertb/misc/shelia/>

HiHAT – High Interaction Honeypot Analysis Tool [online] [cited 9/2/2013]
< http://hihat.sourceforge.net/index.html>

Ι. Κονιάρης ''Ανάλυση Κυβερνοεπιθέσεων με Honeypots Μεσαίας και Χαμηλής Αλληλεπίδρασης'' Πτυχιακή εργασία, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Σχολή Θετικών Επιστημών, Τμήμα Πληροφορικής, Ελλάδα (Οκτώβριος 2012).

[1] IP Addresses: About Networks and Hosts [online] [cited 9/8/2018]
< https://community.fs.com/blog/know-ip-address-and-subnet-mask.html>

[2] What Is Subnetting and Subnet Mask? [online] [cited 9/8/2018]
< https://community.fs.com/blog/know-ip-address-and-subnet-mask.html>

[3] Difference Between TCP/IP and OSI Model [online] [cited 25/3/2016]
< https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html>

[4] TCP/IP Network Administration, 3rd Edition by Craig Hunt [online]
< https://www.oreilly.com/library/view/tcpip-network-administration/0596002971/ch01.html>

[5] information security (infosec) [online] [cited 4/2019]
< https://searchsecurity.techtarget.com/definition/information-security-infosec>

[6] confidentiality, integrity, and availability (CIA triad) [online] [cited 11/2014]
< https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>

[7] Wikipedia. ARP spoofing [online] [cited 11/10/2017]
< https://el.wikipedia.org/wiki/ARP_spoofing>

[8] Wikipedia. Session hijacking [online] [cited 17/5/2019]
< https://en.wikipedia.org/wiki/Session_hijacking>

[9] Wikipedia. DNS spoofing [online] [cited 9/5/2019]
< https://en.wikipedia.org/wiki/DNS_spoofing>

[10] Wikipedia. Malware [online] [cited 26/5/2019]
< https://en.wikipedia.org/wiki/Malware>

[11] L. Spitzner '' Honeypots: Catching the Insider Threat'' [online] [cited 8/12/2003]
< https://pdfs.semanticscholar.org/eece/717fe9d08c12d322f8d8c5cce99b4ff5f806.pdf>.