ΚΕΦΑΛΑΙΟ 1
HONEYPOTS, HONEYNETS

"Μόνο κάποιος που γνωρίζει τις μεθόδους των επιτιθέμενων μπορεί να προστατεύσει κατάλληλα τα συστήματα του..."

Εισαγωγή

Τα υπολογιστικά συστήματα που είναι σήμερα συνδεδεμένα με το διαδίκτυο, δέχονται διαρκώς επιθέσεις από worms, αυτοματοματοποιημένες επιθέσεις και εισβολείς. Θα έλεγε κανείς ότι βρίσκονται πάντα κάτω από ελέγχους (audits) και επιθέσεις που σκοπό έχουν να ανακαλύψουν και να εκμεταλλευτούν ακόμα και το παραμικρό κενό στην αλυσίδα της ασφάλειας. Ένα από τα πιο πρόσφατα εργαλεία στον "πόλεμο" για την αντιμετώπιση των δικτυακών επιθέσεων από κακόβουλους χρήστες και αυτοματοποιημένες επιθέσεις worms και autorooters είναι τα honeypots και τα honeynets.

Ένα honeynet είναι μια συλλογή από συστήματα -τα honeypots-τα οποία προσποιούνται οτι είναι αληθινοί στόχοι, ώστε να δεχτούν επιθέσεις και τελικά να παραβιαστούν. Τα honeypots παρακολουθούνται ώστε να είναι εφικτή η καταγραφή των ενεργειών των επιτιθέμενων και να γνωστοποιούνται οι τεχνικές και τα εργαλεία τα οποία χρησιμοποίησαν για την εισβολή. Είναι χρήσιμα για να αποσπούν και να μπερδεύουν κάποιον από τα υπόλοιπα μηχανήματα ενός δικτύου, να ειδοποιούν για νέους τρόπους επιθέσεων/ευπαθειών, να παρέχουν ανάλυση σε μεγάλο βάθος του τι έγινε κατά τη διάρκεια μιας επίθεσης αλλά και μετά από αυτή. Τα honeynets σε αντίθεση με τα firewalls που εμποδίζουν τους επιτιθέμενους από το να εισβάλλουν σε ένα δίκτυο, λειτουργούν παθητικά στη συλλογή πληροφοριών για τη δράση των blackhats, χρησιμοποιούνται στον τομέα της πρόληψης, της ανίχνευσης, της συλλογής πληροφοριών, έρευνας και εκπαίδευσης.
Σημείωση: Στην πτυχιακή εργασία του Γεωργίου Αλεξανδράτου με τίτλο "Ανάλυση δεδομένων από τη λειτουργία των honeynets στο εργαστήριο islab του ΕΚΕΦΕ ΔΗΜΟΚΡΙΤΟΣ. Μέθοδος, εργαλεία και βασικές έννοιες" [9] υπάρχει πολύ επεξηγηματικό υλικό για τα honeynets.

Τι είναι τα honeypots

Ένας τρόπος για να εντοπίσουμε καινούργιες ευπάθειες συστημάτων -vulnerabilities-είναι

να εγκαταστήσουμε συστήματα σε ένα δίκτυο και να τα παρακολουθούμε, ενώ περιμένουμε ότι κάποια στιγμή θα παραβιαστούν. Αφού τα συστήματα αυτά δεν είναι σχεδιασμένα να έχουν κάποια παραγωγική χρήση, κάθε προσπάθεια για επικοινωνία με αυτά τα συστήματα από το δίκτυο είναι εξορισμού ύποπτη και πρόκειται για προσπάθεια επίθεσης -για παράδειγμα απόπειρα για διείσδυση ή δραστηριότητα worm. Τέτοια συστήματα λέγονται honeypots. Είναι “ιδιαίτερα εποπτευόμενα” υπολογιστικά συστήματα (φυσικά ή εικονικά) τα οποία σκοπεύουν στο να ανιχνευθούν, να δεχτούν επιθέσεις και να “σπάσουν” τελείως. Η αξία τους καθορίζεται από την πληροφορία που μπορεί να εξαχθεί. Τα ίδια τα συστήματα δεν έχουν κάποια αξία για τον διαχειριστή τους μιας και δεν τρέχουν υπηρεσίες κάποιας αξίας και δεν υπάρχουν πολύτιμα δεδομένα. Μια επίθεση που δεν είναι γνωστή μέχρι στιγμής μπορεί να ανιχνευτεί παρακολουθώντας την κίνηση που φεύγει από το honeypot.

Όταν ένα honeypot παραβιάζεται, μελετάμε τον τρόπο που χρησιμοποιήθηκε για την παραβίαση. Ένα honeypot μπορεί να τρέχει οποιοδήποτε λειτουργικό σύστημα και υπηρεσίες, τα οποία θα καθορίσουν πόσο εύκολα θα σπάσει.

Τα honeypots δεν είναι ιδιαίτερα καινούργια ιδέα και χρησιμοποιούνται αρκετό καιρό, ωστόσο η λέξη honeypot είναι καινούργια και εισάγει σε μια νεα μορφή τεχνολογίας που γίνεται ολοένα και πιο σημαντική.

Τι είναι τα honeynets

Τα honeynets είναι δίκτυα αποτελούμενα από συστήματα honeypots τα οποία παρακολουθούνται στενά ώστε να μπορούν να εντοπιστούν και να αναλυθούν οι επιθέσεις που δέχονται τα honeypots. Ένα honeynet συνήθως αποτελείται από διαφορετικού τύπου honeypots, δηλαδή συστήματα με διαφορετικές υπηρεσίες και λειτουργικά συστήματα, ώστε να συγκεντρώνονται ταυτόχρονα δεδομένα από διαφορετικά συστήματα αλλά και να αποτελούν ένα περισσότερο αληθοφανές δίκτυο. Μερικές φορές μάλιστα σχεδιάζονται ώστε να αποτελούν ολοκληρωμένα αντίγραφα δικτύων ή παραγωγικών συστημάτων.

Ο στόχος ενός honeynet είναι να συλλέγει δεδομένα από κάθε δυνατή πηγή, ενώ ταυτόχρονα προστατεύει το δίκτυο με το να περιορίζει τις κακόβουλες κινήσεις από τα κατειλημμένα honeypots. Αυτό γίνεται συνήθως με το να εφαρμόζεται κάποιο φίλτρο στον εξωτερικό router για την εξερχόμενη κίνηση, ώστε αν κατειληφθούν το συστήματα και οι επιτιθέμενοι προσπαθήσουν να κάνουν μια επίθεση denial of service πχ σε κάποιο άλλο δίκτυο, να μην είναι εφικτό.

Διακρίσεις honeypots

Υπάρχουν δυο διακρίσεις για τα διάφορα είδη honeypots: τα φυσικά και τα εικονικά, καθώς επίσης τα υψηλής και τα χαμηλής αλληλεπίδρασης.

- Ένα φυσικό honeypot είναι ένα πραγματικό μηχάνημα με τη δικιά του ip διεύθυνση. Μπορεί να τρέχει οποιοδήποτε λειτουργικό σύστημα -linux, unix, windows, Mac Os, κτλ-και οποιαδήποτε υπηρεσία του ορίσουμε -πχ www, mysql, ftp .

- Επιπλέον μπορεί να ρυθμιστεί ένα υπολογιστικό σύστημα να φιλοξενεί μερικά εικονικά μηχανήματα, δεν πρόκειται δηλαδή για πραγματικά μηχανήματα αλλά για προσομείωση συστημάτων σε κάποιον υπολογιστή. Αυτό προσφέρει πολύ ευκολότερη συντήρηση και λιγότερες φυσικές απαιτήσεις. Για εικονικά honeypots χρησιμοποιούνται το Vmware [2] ή το user-mode linux [3]. Πρόκειται για λογισμικό που επιτρέπει να τρέχουν περισσότερα απο ένα λειτουργικά συστήματα σε ένα μηχάνημα. Με ένα δυνατό σε ισχύ μηχάνημα μπορεί να τρέχουν αρκετά διαφορετικά λειτουργικά συστήματα, το καθένα από τα οποία θα έχει τη δική του ip και μπορούν να δημιουργηθούν ακόμα και αυθαίρετες δικτυακές τοπολογίες.

Με διάκριση την αλληλεπίδραση, δηλαδή το βαθμό δραστηριότητας που επιτρέπεται να έχει ένας επιτιθέμενος σε ένα honeypot, μπορούμε να τα διαιρέσουμε σε χαμηλής και υψηλής αλληλεπίδρασης.

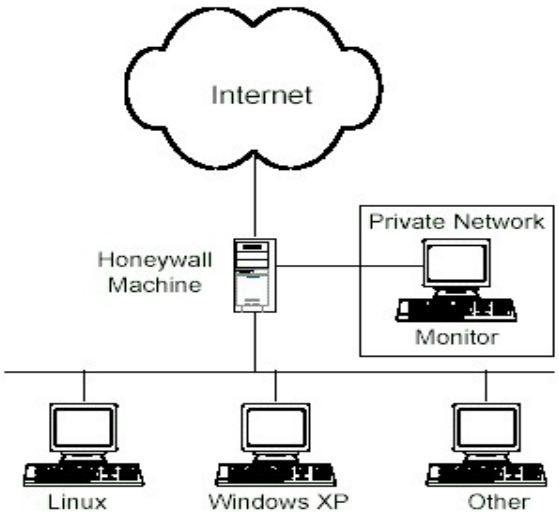
- Τα υψηλής αλληλεπίδρασης honeypots παρέχουν ένα ολόκληρο λειτουργικό σύστημα και υπηρεσίες με τις οποίες ο επιτιθέμενος μπορεί να συνδεθεί. Είναι πραγματικοί υπολογιστές με πραγματικές εφαρμογές που οι επιτιθέμενοι μπορούν να παραβιάσουν και να πετύχουν απόλυτο έλεγχο του συστήματος.

- Αντίθετα τα χαμηλής αλληλεπίδρασης honeypots έχουν περιορισμένες δυνατότητες, καθώς προσομοιώνουν μερικά μόνο μέρη ,πχ τη στοίβα δικτύου. Αυτό που κάνουν είναι να εξομοιώνουν συστήματα και οι δραστηριότητες των επιτιθέμενων περιορίζονται σε αυτό που επιτρέπουν οι εξομοιωμένες υπηρεσίες. Δεν μπορεί να γίνει πλήρες compromise καθώς δεν πρόκειται για πραγματικά συστήματα με πλήρης εφαρμογές.

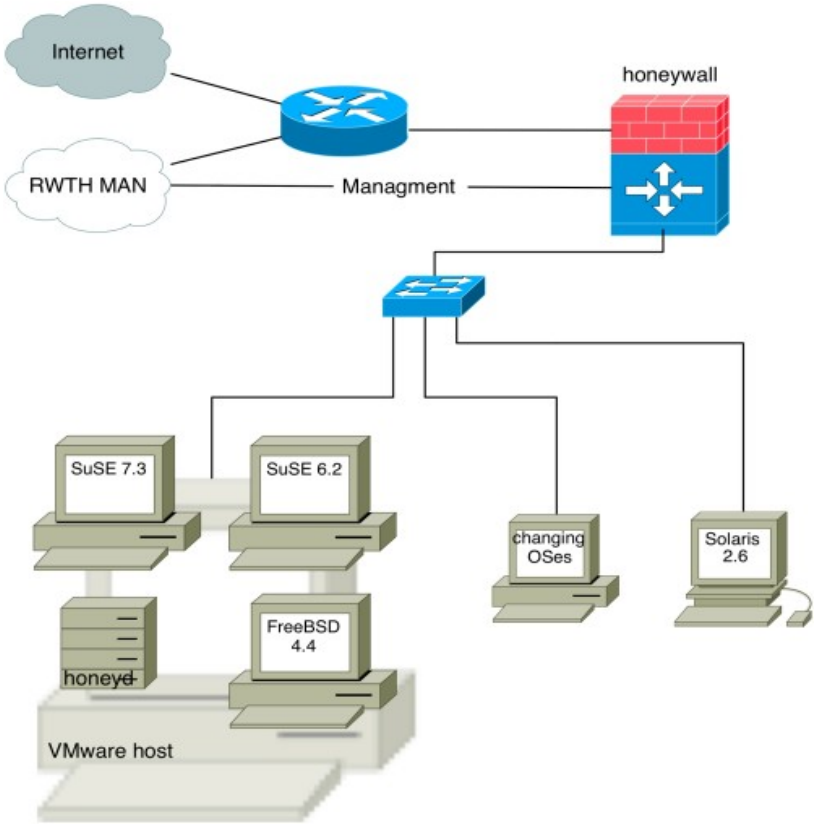
Όταν πρέπει να μπούνε honeypots σε μεγάλο αριθμό διευθύνσεων -πχ C class δίκτυο ή ακόμα και B class τα physical honeypots και τα υψηλής αλληλεπίδρασης δεν αποτελούν επιλογή, καθώς δεν είναι πρακτικά.

Ένα εργαλείο για τη δημιουργία χαμηλής αλληλεπίδρασης honeypots είναι το honeyd. Το honeyd είναι ένα μικρό πρόγραμμα το οποίο δημιουργεί virtual hosts σε ένα δίκτυο με το να προσομοιώνει την TCP/IP στοίβα διαφόρων λειτουργικών συστημάτων και μπορεί να ρυθμιστεί να τρέχει υπηρεσίες. Αυτές οι υπηρεσίες είναι συνήθων μικρά scripts που προσομοιώνουν πραγματικές υπηρεσίες όπως το POP3 ή το SMTP.

Τα υψηλής αλληλεπίδρασης honeypots μπορούν να καταγράψουν μεγαλύτερη πληροφορία από τα χαμηλής αλληλεπίδρασης. Μπορούν να καταγράψουν ολόκληρη τη σύνδεση του επιτιθέμενου με το σύστημα από τη στιγμή της παραβίασης και μετά, το τι έκανε δηλαδή και πως έγινε αυτό, τι προγράμματα εγκατέστησε στο σύστημα κτλ. Πέρα από αυτό όμως τα υψηλής αλληλεπίδρασης honeypots θέλουν πολύ περισσότερη δουλειά για να στηθούν και να συντηρηθούν. Μιας και πρόκειται για πραγματικά συστήματα, αποτελούν κίνδυνο γιατί οι επιτιθέμενοι μπορεί να τα χρησιμοποιήσουν για να πραγματοποιούν από αυτά τις επιθέσεις τους ή αν βλάψουν άλλα συστήματα. Η δουλειά που πρέπει να γίνει σε αυτά είναι σημαντικά περισσότερη.



εικόνα 1.1-ένα δίκτυο honeynet με τρια honeypots



εικόνα 1.2-honeynet με φυσικούς και virtual hosts

Εργαλεία

Αρχικά στήνεται ένα δίκτυο με υπολογιστές που τρέχουν διάφορα λειτουργικά συστήματα, πχ linux, windows, mac κτλ. Τα συστήματα αυτά μπορεί να είναι φυσικά είτε εικονικά. Ο αριθμός τους μπορεί να είναι από δυο-τρια μέχρι πολύ περισσότερα. Τα συστήματα αυτά συνήθως ρυθμίζονται να τρέχουν πολλές υπηρεσίες -web, ftp, sql κτλ-ώστε να υπάρχουν πολλά σημεία εισόδου για το σύστημα. Η καταγραφή των συμβάντων και των επιθέσεων γίνεται με τους εξής τρόπους:

1. Από τα log του firewall βλέπουμε ποιες συνδέσεις έγιναν και μπορούμε να μάθουμε πότε ξεκίνησε μια συγκεκριμένη σύνδεση.

2. Από τα log που αφήνουν οι υπηρεσίες, για παράδειγμα logs από τον apache web server, ή απο τον iis.

3. Με χρήση κάποιου συστήματος IDS, όπως το snort παίρνουμε αυτόματα ειδοποιήσεις όταν συμβαίνουν επιθέσεις. Υπάρχουν διάφορα εργαλεία και front-ends που χρησιμοποιούνται σε συνδυασμό με το snort για να γίνεται πιο αποδοτική

η ανάλυση των logs, όπως το ACID, το demarc κα.

4. Από το αρχείο με τη δικτυακή κίνηση που κατέγραψε κάποιο sniffer το οποίο τρέχει στο δίκτυο. Το sniffer μπορεί να είναι το tcpdump ή οποιοδήποτε άλλο sniffer αλλά όπως θα δούμε στο κεφάλαιο 5 μπορεί να είναι και το ίδιο το snort.

5. Στο linux υπάρχει η δυνατότητα να παρακολουθήσουμε το τι έκανε ο επιτιθέμενος στο σύστημα αφότου απόκτησε πρόσβαση με το να εγκαταστήσουμε λογισμικό που πιάνει τις πληκτρολογήσεις του. Το πιο γνωστό εργαλείο που χρησιμοποιείται για τη δουλειά αυτή είναι το Sebek. Το sebek λειτουργεί ως client/server σύστημα, τρέχει στο honeypot που μας ενδιαφέρει και στέλνει τα δεδομένα σε κάποιο δικό μας server μέσω του syslog, ώστε ένας επιτιθέμενος να μην μπορεί να αντιληφθεί την ύπαρξη του. Το sebek μπορεί έτσι να πιάνει τη δραστηριότητα του επιτιθέμενου στο σύστημα, το τι προσπαθεί να κάνει σε άλλα συστήματα, καθώς επίσης και τα διάφορα αρχεία που κατεβάζει. Εφόσον το sebek εγκαθίσταται στο σύστημα, μπορεί να καταγράψει μια σύνδεση ssh, την οποία το ids δεν μπορεί να καταλάβει.

The global honeynet project

Ιδρυμένο το 1999, το Honeynet Project [1] είναι μια μη κερδοσκοπική ερευνητική οργάνωση στην οποία επαγγελματίες της ασφάλειας κάνουν έρευνα στον τομέα της ασφάλειας υπολογιστών. Το honeynet project είναι ένα group επαγγελματιών ερευνητών της ασφάλειας IT που στήνουν δίκτυα honeynets στο internet και παρακολουθούν πως παραβιάζονται με σκοπό να μάθουν τα εργαλεία, τις τακτικές και τα κίνητρα των δικτυακών εισβολέων και των blackhats και να τα διαθέσουν τη γνώση στο διαδίκτυο ελεύθερα για όλους. Ο όρος blackhat χρησιμοποιείται για να περιγράψει έναν επιτιθέμενο ο οποίος χρησιμοποιεί τις δυνατότητες του για μη ηθικούς ή καταστροφικούς σκοπούς.
Εισηγητής του καινούργιου αυτού όρου περιγραφής τέτοιων συστημάτων αλλά και ιδρυτής του honeynet project είναι ο Lance Spitzner. Στο honeynet project συμμετέχουν πολλοί διάσημοι ερευνητές αλλά και hackers, όπως οι George Kurtz (Foundstone), Elias Levy (securityfocus.com), Dug Song (dsniff writer), Fyodor (nmap writer), Jay Beale (Bastille linux), Rain Forest Puppy και άλλοι, ενώ τα ενεργά honeynet projects αυτή τη στιγμή είναι τα εξής:

- Chinese Honeynet Project, The Spanish Honeynet Project, SIG^2 Internet Weather Forecast Centre, German Honeynet Project, Portugal Honeynet Project, Ga Tech Honeynet Project, French Honeynet Project, Italian Honeynet Project, Pakistan Honeynet

Project, West Point Honeynet Project, UK Honeynet Project, Honeynet Project at the University of Texas at Austin, Brazilian Honeynet Project, Azusa Pacific University Honeynet, NetForensics Honeynet, Internet Systematics Lab Honeynet Project – Greece, Paladion Networks Honeynet Project – India, Norwegian Honeynet Project, Florida HoneyNet Project

Φυσικά, πέρα απο τα επίσημα honeynets του honeynet project υπάρχουν και τα πολύ περισσότερα honeypots και honeynets που έχουν στηθεί απο επιχειρήσεις και οργανισμούς για να ενημερώσουν τους υπαλλήλους τους, αλλά και κυρίως για να έχουν εικόνα του τι συμβαίνει στο δίκτυο τους.

Οι στόχοι του project αναλυτικά είναι οι εξής:

- **Να ευαισθητοποιήσει σε θέματα ασφάλειας δικτύων**

  Το project στοχεύει στο να ενημερώσει τους χρήστες του internet για τους κινδύνους και τις απειλές που υπάρχουν σήμερα. Αυτό το καταφέρνει με το να στήνει πραγματικά δίκτυα και να μελετάει πως αυτά παραβιάζονται από πραγματικούς επιτιθέμενους. Όλα τα αποτελέσματα από την έρευνα δημοσιεύονται στο internet ώστε να μπορεί να τα δει οποιοσδήποτε, ενώ είναι γραμμένα σε κατανοητή γλώσσα ακόμα και για αρχαρίους και περιέχουν πολλές λεπτομέρειες.

  Οι περισσότεροι χρήστες του internet δεν γνωρίζουν για τους κινδύνους που αντιμετωπίζουν. Μάλιστα, πολλές φορές δεν ξέρουν ότι το σύστημα τους είναι ήδη παραβιασμένο! Ένας επιτιθέμενος τις περισσότερες φορές και ανάλογα με το επίπεδο του, θα προσπαθήσει να καλύψει τα ίχνη της παραβίασης ώστε να συνεχίσει να έχει πρόσβαση. Επιπλέον, τα περισσότερα σημερινά λειτουργικά συστήματα σε μια default εγκατάσταση έρχονται με ήδη υπάρχοντα προβλήματα ασφάλειας. Μέχρι να κάνει τις απαραίτητες ενέργειες ο χρήστης για να τα ασφαλίσει, πχ μέχρι να κατεβάσει και να εγκαταστήσει κάποιο patch, το σύστημα μπορεί να παραβιαστεί και να μην το καταλάβει ο χρήστης. Τα honeynets βοηθάνε στην ευαισθητοποίηση σε θέματα ασφάλειας με το να κάνουν ορατούς αυτούς τους κινδύνους. Πολλές φορές οι χρήστες υπολογιστών ξεγέλιουνται νομίζοντας ότι κανείς δεν θα προσέξει το σύστημα τους και δεν θα θελήσει να ασχοληθεί με αυτό. Το honeynet project έχει αποδείξει ότι ένα σύστημα που τρέχει την default εγκατάσταση του λογισμικού του συστήματος και συνδέεται με το internet, θα δεχτεί πολλαπλά scans και τελικά θα παραβιαστεί μετά από κάποιο χρόνο.

- **Έρευνα σε παλιές αλλά και καινούργιες τεχνικές**

Τα honeynets παρέχουν την τεχνολογία και τις μεθόδους για να συγκεντρώνεται πληροφορία για τις επιθέσεις στο διαδίκτυο. Η ανάλυση των δεδομένων που συγκεντρώθηκαν μπορεί να βοηθήσει τους administrators να προστατεύσουν καλύτερα το δίκτυο τους. Με την ανάλυση της συμπεριφοράς ενός επιτιθέμενου, μπορούμε να καταλάβουμε πως έγινε η επίθεση, ποια ήταν τα κίνητρα, πως επιχείρησε να χρησιμοποιήσει το σύστημα μας και τι προσπάθησε να κάνει. Μιας και οι συνδέσεις που γίνονται καταγράφονται, τα συστήματα honeypots επίσης μπορούν να πιάσουν κάποιο νεο τύπο επίθεσης, που δεν είναι γνωστός μέχρι στιγμής.

- **Ενεργός δικτυακή προστασία**

Τα honeynets μπορούν επίσης να αποτελέσουν μέρος της προστατευτικής υποδομής ενός δικτύου, γιατί μπορούν να μπερδέψουν τους επιτιθέμενους και να τους αποθαρρύνουν από το να συνεχίσουν τη διείσδυση στο δίκτυο. Επίσης, τα honeypots μπορούν να μας ειδοποιούν για τα μολυσμένα συστήματα στο δίκτυο μας, περίπτωση που αναλύεται σε επόμενο κεφάλαιο. Αυτό ισχύει επειδή μιας και τα honeypots δεν έχουν παραγωγική χρήση, όλες οι συνδέσεις είναι εξορισμού ύποπτες και δεν υπάρχουν τα false positives που θα βγάλει κάποιο ids. Σε ορισμένες περιπτώσεις τα honeypots μας ειδοποιούν για τα μολυσμένα συστήματα στο δίκτυο μας πολύ εγκυρότερα από τα ids. Έτσι μπορούμε να ειδοποιήσουμε τους διαχειριστές των συστημάτων αυτών για να διορθώσουν τα κενά στην ασφάλεια τους. Τέλος η τεχνολογία bait'n'switch αν και ελάχιστα χρησιμοποιείται σήμερα, αξίζει παρόλαυτα να τη δούμε αναλυτικότερα: Το bait'n'switch πραγματοποιείται σαν μια προέκταση του snort. Όποτε μια επιτυχημένη επίθεση εντοπίζεται ότι συμβαίνει, το ids φιλτράρει την επίθεση και η κίνηση του επιτιθέμενου προωθείται σε ένα σύστημα όμοιο με αυτό που δέχτηκε την επίθεση. Τη διαδικασία αυτή δεν την καταλαβαίνει ο επιτιθέμενος. Έτσι το πραγματικό σύστημα προστατεύεται από την επίθεση και η αλληλεπίδραση του επιτιθέμενου με το honeypot σύστημα μπορεί να μελετηθεί περισσότερο. Το σύστημα βέβαια αντιδρά μόνο σε επιθέσεις για τις οποίες έχει κανόνες ανανεωμένους.

- **Εκπαίδευση πάνω στην ασφάλεια**

Ένα δίκτυο με honeypots μπορεί να χρησιμοποιηθεί από άτομα που θέλουν να μελετήσουν στην πράξη πώς συμβαίνουν οι δικτυακές επιθέσεις, μέσα από ένα ρεαλιστικό περιβάλλον και χωρίς τους κινδύνους της παραβίασης παραγωγικών συστημάτων. Έτσι τα άτομα αυτά μπορούν να αναλύσουν τα δεδομένα από τις επιθέσεις. Σε κάποια πανεπιστήμια ήδη χρησιμοποιούνται honeynets για τη διδασκαλία μαθημάτων

ασφάλειας δικτύων.

Επιτυχίες του honeynet project

Το honeynet project από την αρχή της λειτουργίας του έχει εκδώσει πλήθος από άρθρα γύρω από την ασφάλεια δικτύων, τα οποία πέρα από το γεγονός ότι είναι πολύ αναλυτικά, είναι γραμμένα σε απλό και επεξηγηματικό ύφος, ώστε να μπορούν να τα κατανοήσουν και σχετικά αρχάριοι στο χώρο της ασφάλειας δικτύων. Τα άρθρα αυτά είναι πραγματικά case studies από στοιχεία που μάζεψαν με κάποιο honeynet. Ακόμα και στο internet με τον τεράστιο όγκο της πληροφορίας που υπάρχει, είναι δύσκολο να βρεθούν τόσο καλογραμμένα άρθρα, όπως αυτά που έχουν βγει από το honeynet project για το spam, τα botnets, το phishing, τις αυτοματοποιημένες δικτυακές επιθέσεις και τα worms, αλλά και για περιπτώσεις παραβιασμένων συστημάτων με σκοπό να μάθουμε τι έκαναν οι επιτιθέμενοι.

Ένα από τα άρθρα [10] από το project (Δεκέμβριος 2004) δείχνει ότι ο μέσος χρόνος στον οποίο περιμένουμε ότι ένα μη ασφαλισμένο Linux σύστημα θα παραβιαστεί, ένα σύστημα με default εγκατάσταση δηλαδή χωρίς περασμένα patches, είτε από επιτιθέμενους είτε από αυτοματοποιημένες επιθέσεις και worms είναι 3 μήνες. Ο αντίστοιχος χρόνος για ένα μη ασφαλισμένο σύστημα windows δεν μετριέται σε μήνες, αλλά σε ώρες! Σε κάποιες περιπτώσεις μάλιστα τα windows συστήματα παραβιάστηκαν μερικά λεπτά αφού συνδέθηκαν με το internet! Το γεγονός αυτό εξηγείται από την μεγάλη εξάπλωση των worms sasser, mydoom και netsky το διάστημα εκείνο. Τα ίδια συμπεράσματα επιβεβαιώνονται και από τη Symantec [11] και από το Internet Storm Center [12].

Υπάρχουν περιπτώσεις όπου τα honeynets βοήθησαν να ανακαλυφθεί κάποιο vulnerability που κυκλοφορούσε στο internet χωρίς να είναι γνωστή η παρουσία του. Για παράδειγμα, τον Ιανουάριο του 2002 τα δεδομένα από κάποιο honeynet επέτρεψαν την αναγνώριση ενός exploit για μια vulnerability στην υπηρεσία dtspcd του CDE [13]. Honeynets επίσης έχουν χρησιμοποιηθεί για την παρακολούθηση συζητήσεων στο IRC και την εύρεση botnets. Τα botnets είναι δίκτυα από εκατοντάδες ή και χιλιάδες υπολογιστές παραβιασμένους -τα λεγόμενα zobiesστα οποία έχει εγκατασταθεί λογισμικό ώστε να υπακούουν όλα μαζί με εντολές που παίρνουν από το IRC. Χρησιμεύουν στους επιτιθέμενους για μαζικά scannings και distributed denial of service. Έχουν καταγραφεί ακόμα και αγορές-πωλήσεις δικτύων botnets! Το Honeynet Project στο Azusa Pacific University ανακάλυψε ένα botnet με περισσότερα από 15,000 συστήματα.

Άλλες επιτυχίες με τη χρήση honeypots περιλαμβάνουν την εύρεση καναλιών IRC απο

οργανωμένα κυκλώματα απάτης μέσω πιστωτικών καρτών.

Προβλήματα που πιθανόν να προκύψουν από ένα honeynet

Πέρα από τα πλεονεκτήματα που προσφέρει η εγκατάσταση honeypots και honeynets, πρέπει να ληφθούν υπόψιν και τα προβλήματα που μπορεί να δημιουργήσουν, ώστε να γίνει σωστή αποτίμηση των πλεονεκτημάτων και μειονεκτημάτων στο περιβάλλον όπου σκοπεύει να γίνει η εγκατάσταση.

- Το να μπουν σε ένα δίκτυο honeypots σημαίνει ότι προστίθονται συστήματα με χαλαρή ασφάλεια ή και καθόλου ασφαλισμένα, έτσι ολόκληρη η ασφάλεια του δικτύου πιθανόν να κινδυνεύει.
- Επιπλέον, για όποιες παραβιάσεις γίνουν με τα honeypots σαν ενδιάμεσα σημεία (jumping points) για τους επιτιθέμενους, ο υπεύθυνος του δικτύου μπορεί να αντιμετωπίσει νομικά προβλήματα. Στη σελίδα του honeynet project πάντως υπάρχει άφθονο υλικό για το στήσιμο ενός δικτύου με διακριτές περιοχές και υποδίκτυα, ώστε η παραβίαση των honeypots -που είναι άλλωστε και ο στόχος να μην δημιουργεί προβλήματα στο υπόλοιπο δίκτυο.
- Επίσης είναι σημαντικό ότι περιορίζονται αυστηρά οι πόροι των honeypots προς τα έξω, όπως η εξερχόμενη κίνηση . Έτσι αποτρέπεται ένα honeypot απο το να χρησιμοποιηθεί για denial of service σε εξωτερικά συστήματα ή να πραγματοποιήσει επιθέσεις. Ενδιαφέρει μόνο η αλληλεπίδραση με τον επιτιθέμενο και να μάθουμε τι προσπαθεί να κάνει και όχι απαραίτητα να το κάνει!
- Η παρακολούθηση των κινήσεων του επιτιθέμενου χωρίς τη γνώση του είναι ένα δύσκολο θέμα απο την πλευρά ηθικής αλλά και για νομικούς λόγους. Η νομοθεσία που ισχύει στις ΗΠΑ, μια απο τις πιο αυστηρές νομοθεσίες παγκοσμίως (ιδιαίτερα απο 11/9 και μετά, με το “ανατριχιαστικό” Patriot act) ορίζει ως παγίδευση το εξής:

“ένα άτομο παγιδεύεται όταν ωθείται ή παραπλανείται από τις δυνάμεις του νόμου να διαπράξει ένα έγκλημα το οποίο δε σκόπευε να κάνει”.

Ο ορισμός τίποτα δεν έχει να κάνει με τις ενέργειες και τους στόχους του honeynet project. Η ομάδα δεν ενεργεί κάτω από τον έλεγχο του νόμου και κυρίως δεν έχει σαν στόχο την καταδίκη των επιτιθέμενων. Τα honeynets σχεδιάζονται να μοιάζουν με πραγματικά, παραγωγικά συστήματα και καμιά κίνηση δεν γίνεται για να πείσουν επιτιθέμενους να τους επιτεθούν. Αντίθετα, οι επιτιθέμενοι είναι αυτοί που εντοπίζουν και επιτίθενται στα

συστήματα αυτά. Τα honeypots παρακολουθούνται όχι για να εντοπιστούν οι επιτιθέμενοι, αλλά για να μελετηθούν οι κινήσεις τους, οι τρόποι που πραγματοποιούν μια επίθεση και τα εργαλεία τους, ώστε να υπάρχει η γνώση για να μπορούν να αποτραπούν στα πραγματικά συστήματα.

ΣΗΜΕΙΩΣΕΙΣ – ΠΑΡΑΠΟΜΠΕΣ

[1] http://www.honeynet.org το site toy honeynet

[2] http://www.vmware.com

[3] user mode linux http://www.cert.org/advisories/CA-2002-01.html

[4] sebek http://www.honeynet.org/tools/sebek

[6] The honeynet project, Tools for Honeynets, http://honeynet.org/tools

[7] “Μελέτη των επιθέσεων που στηρίζονται σε πακέτα με ψευδή IP διεύθυνση αποστολέα (IP spoofing)”, πτυχιακή εργασία του Ιωάννη Παπαπάνου, διαθέσιμη online στο http://www.islab.demokritos.gr

[8] “ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ” πτυχιακή εργασία του Κώστα Μάγκου και Άρη Νιξαρλίδη, διαθέσιμη online στο http://www.islab.demokritos.gr

[9]”Ανάλυση δεδομένων από τη λειτουργία των honeynets στο εργαστήριο islab του ΕΚΕΦΕ ΔΗΜΟΚΡΙΤΟΣ. Μέθοδος, εργαλεία και βασικές έννοιες” πτυχιακή εργασία του Γεωργίου Αλεξανδράτου, διαθέσιμη online στο http://www.islab.demokritos.gr

[10] Know Your Enemy:Trend Analysis, the Honeynet project Trend:Life expectancy increasing for unpatched or vulnerable Linux deployments

[11] Symantec Internet Security Threat Report , January 1-June 30 2004

[12] Internet Storm Center-http://isc.sans.org/survivalhistory.php

[13] dtspcd exploit ,http://www.cert.org/advisories/CA-2002-01.html