Κεφάλαιο 1

Εισαγωγή

Honeypots – Honeynets

Εισαγωγή

Το Πρόβλημα

Ο αυξανόμενος αριθμός επιθέσεων στο internet και η ανάγκη για την αντιμετώπιση τους δημιούργησε την ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο παραγωγής. Αξιοποιούμε την τεχνική αναφορά του εργαστηρίου **Internet Systemetics Lab - "Βασικές έννοιες επιθέσεων"** Γ. Βιδάκης, Γ. Παπαπάνος 5/11/2002, για την αρχική μας είσοδο στο πρόβλημα**.** Αν ρίξουμε μια ματιά σε δικτυακούς τόπους όπως τα: http://www.securityfocus.org , http://isc.incidents.org/, http://www.cert.org και σε άλλες παρόμοιες ιστοσελίδες με θέμα security και επιθέσεις, θα παρατηρήσουμε ότι ο αριθμός επιθέσεων όπως και η ανακάλυψη και η εκμετάλλευση νέων ευπαθειών τόσο των εφαρμογών όσο και του λειτουργικού, αυξάνονται συνεχώς.

Η γνώση, για τις εξωτερικές ή εσωτερικές επιθέσεις και τα ιδιαίτερα χαρακτηριστικά τους, έρχεται από την επεξεργασία και ανάλυση των δεδομένων που συλλέγονται, κατά την παρακολούθηση των κινήσεων των επιτιθέμενων ή αλλιώς **blackhats**. Η συλλογή αυτών των δεδομένων διευκολύνεται χρησιμοποιώντας εξειδικευμένες συσκευές, τα **honeypots**.

Ορισμός Honeypots

Τα **honeypots**, είναι συστήματα που έχουν σαν σκοπό να τραβήξουν την προσοχή των επιτιθέμενων και να καταγράψουν τις ενέργειές τους.

Τα **Honeypots** είναι μια σχετικά νέα και ιδιαίτερα δυναμική τεχνολογία. Αυτή η τεχνολογία έχει το χαρακτηριστικό να εξελίσσεται συνεχώς, γι΄ αυτό είναι δύσκολο να την καθορίσουμε ακριβώς. Τα **honeypots,** δεν συμβάλουν ενεργά στην καταπολέμηση των επιτιθέμενων όπως άλλες τεχνολογίες, σαν τα **firewalls** και τα **συστήματα ανίχνευσης επιθέσεων (Intrusion detection systems - IDS)**, οι οποίες είναι ευκολότερο να καθοριστούν

και να κατανοηθούν δεδομένου ότι λύνουν συγκεκριμένα προβλήματα. Τα **firewalls** είναι μια τεχνολογία πρόληψης είναι πύλες δικτύων που κρατούν τους επιτιθέμενους έξω από αυτά . Τα συστήματα ανίχνευσης επιθέσεων (IDS) είναι μια τεχνολογία ανίχνευσης. Ο σκοπός τους είναι να ανιχνεύσουν και να προειδοποιήσουν τους επαγγελματίες ασφάλειας για μη εξουσιοδοτημένη ή κακόβουλη δραστηριότητα. Τα **Honeypots** λειτουργούν παθητικά στην συλλογή πληροφοριών για την δράση των **blackhats**, χρησιμοποιούνται στον τομέα της πρόληψης, της ανίχνευσης, της συλλογής πληροφοριών, έρευνας και εκπαίδευσης.

Θα δούμε ότι τα **honeypots** είναι μια σύνθετη τεχνολογία η οποία δεν ενεργεί στην «Πρώτη γραμμή» εναντίων των **blackhat,** παρά μας χρησιμεύει στην παρακολούθηση των κακόβουλων ενεργειών των επιτιθέμενων ώστε να αποκτούμε-βελτιώνουμε τις γνώσεις μας, για τις συνήθειες και τον τρόπο λειτουργίας τους. Τελικά κατορθώνουμε να βελτιώνουμε τις άμυνες μας εναντίων τους, ή ακόμα και να δημιουργούμε νέες.

Η λίστα των ειδικών στα **Honeypots** honeypots@sourceforge.net, κατέληξε στον παρακάτω ορισμό.

Ορισμός:

*"Ένα **honeypot** είναι ένας πόρος πληροφοριακών συστημάτων του οποίου η αξία έγκειται στην μη εξουσιοδοτημένη ή παράνομη χρήση του πόρου αυτού ."*

Δηλαδή τα **honeypots** είναι μια τεχνολογία της οποίας η αξία εξαρτάται από αυτούς που αλληλεπιδρούν με αυτά. Κανένας δεν έχει λόγο να χρησιμοποιεί ή να αλληλεπιδρά με τα **honeypots,** άρα οποιεσδήποτε συναλλαγές ή αλληλεπιδράσεις με ένα **honeypot** είναι ύποπτες.

Ένα **honeypot** δεν έχει καμία αξία ως σύστημα -παραγωγής, δεν κάνει καμία πραγματικά παραγωγική εργασία όπως η αποθήκευση και επεξεργασία δεδομένων. Οποιεσδήποτε συναλλαγές επεξεργασμένες, οποιαδήποτε προσπάθεια για logins, ή οποιαδήποτε πρόσβαση σε αρχεία δεδομένων σε ένα **honeypot** είναι πλέον πιθανές κακόβουλες ή μη εξουσιοδοτημένες

δραστηριότητες. Παραδείγματος χάριν, ένα σύστημα **honeypot** μπορεί να εγκαταστηθεί σε ένα εσωτερικό δίκτυο. Αυτό το **honeypot** δεν θα είχε καμία αξία παραγωγής και κανένας στον οργανισμό δεν πρέπει να το χρησιμοποιεί. Θα μπορούσε να φαίνεται σαν ένας κεντρικός υπολογιστής αρχείων, ένας κεντρικός υπολογιστής δικτύου, ή ακόμα και ο τερματικός σταθμός ενός υπαλλήλου. Εάν κάποιος αλληλεπιδρά με αυτό το σύστημα, εξετάζει πιθανότατα για τις ευπάθειες ή προσπαθεί να βρει δεδομένα.

Στην πραγματικότητα, ένα **honeypot** δεν είναι απαραίτητο να είναι ένας υπολογιστής. Μπορεί να είναι οποιοσδήποτε τύπος ψηφιακής οντότητας που δεν έχει καμία αξία παραγωγής. Παραδείγματος χάριν, ένα νοσοκομείο θα μπορούσε να δημιουργήσει ένα ψεύτικο σύνολο ηλεκτρονικών αρχείων ασθενών επονομαζόμενων ΚΩΣΤΗΣ ΣΤΕΦΑΝΟΠΟΥΛΟΣ Επειδή αυτά τα αρχεία είναι **honeypots**, κανένας δεν πρέπει να έχει πρόσβαση ή να αλληλεπιδρά με αυτά. Τα αρχεία αυτά θα μπορούσαν έπειτα να καταχωρηθούν στη βάση δεδομένων ασθενών ενός νοσοκομείου ως τμήμα **honeypot**. Εάν οποιοσδήποτε υπάλληλος ή επιτιθέμενος προσπαθήσει να αποκτήσει πρόσβαση σε αυτά τα αρχεία, τότε αυτό θα έδειχνε την μη εξουσιοδοτημένη δραστηριότητα επειδή κανένας δεν θα έπρεπε να τα χρησιμοποιεί. Εάν κάποιος ή κάτι επιδιώξει πρόσβαση σε αυτά τα αρχεία, τότε έχει κανονιστεί να παραγάγουν μια ειδοποίηση (**alert**).

Τύποι Honeypots

Για να καταλάβουμε καλύτερα τους τύπους των **honeypots**, μπορούμε να τα διαιρέσουμε σε δύο γενικές κατηγορίες: *χαμηλής αλληλεπίδρασης* και *υψηλής αλληλεπίδρασης*. Η αλληλεπίδραση είναι ο βαθμός δραστηριότητας που επιτρέπεται να έχει ένας επιτιθέμενος σε ένα **honeypot**. Όσο περισσότερη αλληλεπίδραση επιτρέπει ένα **honeypot**, τόσο περισσότερα μπορεί να κάνει ο επιτιθέμενος με το **honeypot**. Τα χαμηλής-αλληλεπίδρασης **honeypots** έχουν περιορισμένες δυνατότητες, ενώ τα υψηλής-αλληλεπίδρασης **honeypots** παρέχουν πολύ περισσότερες δυνατότητες παραπλάνησης του επιτιθέμενου μιας και προσφέρουν ένα πλήρες σύστημα, παρόμοιο με σύστημα παραγωγής.

Χαμηλής-αλληλεπίδρασης Honeypots

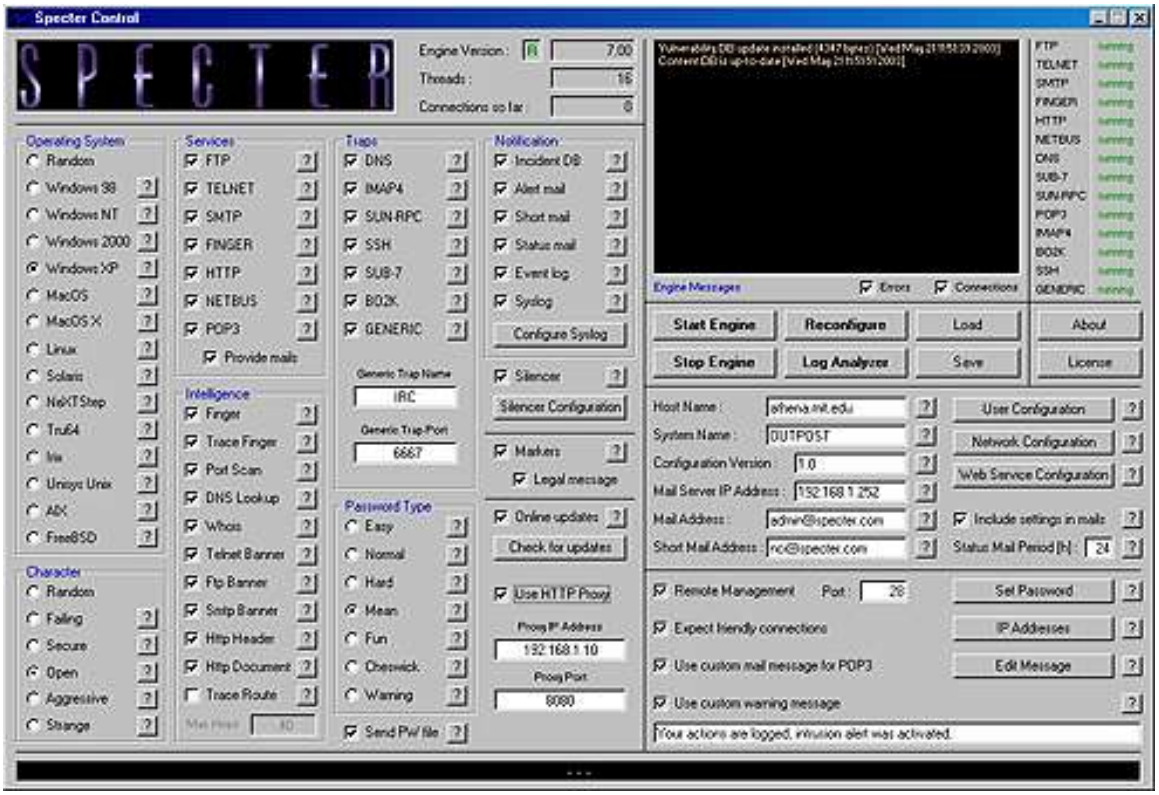
Τα χαμηλής-αλληλεπίδρασης **honeypots** λειτουργούν βασικά με εξομοίωση *συστημάτων (emulating systems)* και *υπηρεσιών (emulating services)*. Οι δραστηριότητες των επιτιθεμένων περιορίζονται σε αυτό που επιτρέπουν οι εξομοιωμένες υπηρεσίες. Παραδείγματος χάριν, το BackOfficer Friendly **honeypot** που παρουσιάζεται στην Εικόνα 1-1 είναι ένα εξαιρετικά απλό **honeypot** που μιμείται επτά διαφορετικές υπηρεσίες. Οι επιτιθέμενοι περιορίζονται πολύ σε αυτό που μπορούν να κάνουν με το, βασισμένο στις εξομοιωμένες υπηρεσίες, honeypot. Κατ' ανώτατο όριο, οι επιτιθέμενοι μπορούν να συνδέθουν με το honeypot και να εκτελέσουν μερικές βασικές εντολές.

Εικόνα 1-1

- Σε αυτό το σχήμα, βλέπετε το User interface ενός πολύ απλού honeypot αποκαλούμενου BackOfficer Friendly. Αυτό το honeypot εκτελεί μόνο μια πολύ βασική αυξομείωση για επτά διαφορετικές υπηρεσίες.

Τα χαμηλής-αλληλεπίδρασης **honeypots** είναι περισσότερο διαδεδομένα επειδή έρχονται προ-διαμορφωμένα με ποικίλες επιλογές για το **administrator**. Αρκεί μόνο να επιλέξετε και να κάνετε κλικ, και έχετε αμέσως ένα **honeypot** με το λειτουργικό σύστημα, τις υπηρεσίες, και τη

συμπεριφορά που θέλετε, όπως φαίνεται στην Εικόνα 1-2 όπου βλέπετε το User Interface τον Specter, ένα χαμηλής-αλληλεπίδρασης honeypot. Το Specter είναι ένα εμπορικό honeypot για Windows. Μπορεί να αυξομειώσει μέχρι 13 διαφορετικά λειτουργικά συστήματα και, να ελέγχει 14 διαφορετικές υπηρεσίες. Τα User interfaces καθιστούν την ανάπτυξη των honeypots πολύ απλή, δεδομένου ότι πρέπει μόνο να κάνετε κλίκ στις υπηρεσίες που θέλετε να ελέγχετε και το πώς θέλετε να συμπεριφέρεται. το **honeypot** .Τα χαμηλής-αλληλεπίδραση **honeypots** επίσης διατρέχουν ελάχιστο κίνδυνο, δεδομένου ότι οι εξομοιωμένες υπηρεσίες περιορίζουν τον επιτιθέμενο, στο τι μπορεί και τι δεν μπορεί να κάνει. Δεν υπάρχει κανένα πραγματικό λειτουργικό σύστημα για τον επιτιθέμενο ώστε να φορτώσει κάποια **toolkits** (συλλογές από εργαλεία) , ούτε υπάρχουν εκεί οποιεσδήποτε υπηρεσίες που να είναι σε θέση να παραβιαστούν πραγματικά.



Εικόνα 1-2 - Specter χαμηλής αλληλεπίδρασης honeypot

Εντούτοις, οι εξομοιωμένες υπηρεσίες περιορίζονται στο πλήθος των πληροφοριών που μπορούν να συλλάβουν, δεδομένου ότι οι επιτιθέμενοι έχουν όρια ως προς αυτό που μπορούν να κάνουν. Επίσης, οι εξομοιωμένες υπηρεσίες δουλεύουν καλύτερα με γνωστή συμπεριφορά ή αναμενόμενες επιθέσεις. Όταν οι επιτιθέμενοι κάνουν κάτι άγνωστο ή απροσδόκητο, τα χαμηλής-αλληλεπίδρασης **honeypots** έχουν δυσκολία να καταλάβουν τις ενέργειες του επιτιθέμενου,ώστε να αποκρίνονται κατάλληλα, ή να καταγράφουν τη δραστηριότητα. Μερικά παραδείγματα χαμηλής-αλληλεπίδρασης **honeypots** είναι το **Honeyd**, το **Specter**, και **KFSensor**.

Υψηλής-αλληλεπίδρασης Honeypots

Τα υψηλής-αλληλεπίδρασης **honeypots** είναι πολύ διαφορετικά από τα χαμηλής-αλληλεπίδρασης **honeypots** δεδομένου ότι παρέχουν ολόκληρα λειτουργικά συστήματα και εφαρμογές για να αλληλεπιδράσουν οι επιτιθέμενοι πάνω σε αυτά. Τα υψηλής-αλληλεπίδρασης **honeypots** δεν εξομοιώνουν αλλά, είναι πραγματικοί υπολογιστές με πραγματικές εφαρμογές που δίνουν στους επιτιθέμενους την δυνατότητα να τα παραβιάσουν. Τα πλεονεκτήματα που παρέχονται από τα υψηλής-αλληλεπίδρασης **honeypots** είναι τεράστια. Κατ' αρχάς , έχουν ως σκοπό να καταγράψουν όσο γίνεται μεγαλύτερο όγκο πληροφοριών. Όχι μόνο μπορούν να ανιχνεύσουν τους επιτιθέμενους που εξετάζουν ένα σύστημα, επιτρέπουν επίσης στους επιτιθέμενους να παραβιάσουν μια υπηρεσία και να αποκτήσουν πρόσβαση στο λειτουργικό σύστημα. Μέσα από ένα παραβιασμένο σύστημα μπορούμε να αποκαλύψουμε τα **rootkits** των επιτιθεμένων διότι τα φορτώνουν επάνω στο σύστημα, να αναλύσουμε τις πληκτρολογήσεις τους όταν αλληλεπιδρούν με το σύστημά μας , όταν μιλούν με άλλους επιτιθέμενους και οποιαδήποτε άλλη αλληλεπίδραση έχουν. Κατά συνέπεια, μπορείτε να μάθετε τα κίνητρα των επιτιθεμένων, τα επίπεδα ικανότητας, την οργάνωση, και άλλες κρίσιμες πληροφορίες.

Επίσης, δεδομένου ότι τα υψηλής-αλληλεπίδρασης **honeypots** δεν εξομοιώνουν, έχουν ως σκοπό να συλλάβουν τη νέα, άγνωστη, ή απροσδόκητη συμπεριφορά. Κατ' επανάληψη, τα υψηλής-αλληλεπίδρασης **honeypots** έχουν συλλάβει δραστηριότητα που εμφανίζεται για πρώτη

φορά . Εντούτοις, αυτές οι τεράστιες ικανότητες έχουν κάποιο τίμημα. Κατ' αρχάς, τα υψηλής-αλληλεπίδρασης **honeypots** θέτουν ένα υψηλό επίπεδο κινδύνου. Δεδομένου ότι στους επιτιθέμενους παρέχονται πραγματικά λειτουργικά συστήματα για να αλληλεπιδράσουν πάνω σ' αυτά. Τα ίδια τα **honeypots** μπορούν να χρησιμοποιηθούν ως μέσα για να επιτεθούν ή να βλάψουν άλλα μη-**honeypots** συστήματα. Δεύτερον, τα υψηλής-αλληλεπίδρασης **honeypots** είναι πολύ σύνθετα. Δεν εγκαθιστάτε απλά το λογισμικό και έχετε αμέσως ένα **honeypot**. Αντί αυτού, πρέπει να χτίσετε και να διαμορφώσετε τα πραγματικά συστήματα για τους επιτιθέμενους για να αλληλεπιδράσουν με αυτά. Επίσης, πολλή πολυπλοκότητα προστίθεται επειδή προσπαθούμε να ελαχιστοποιήσουμε τον κίνδυνο οι επιτιθέμενοι χρησιμοποιώντας τα **honeypots** να κάνουν ζημιά πραγματοποιώντας επιθέσεις σε άλλα συστήματα.

Honeynets

Το **honeynet** είναι ένας ακόμη τύπος **honeypot** και μάλιστα είναι από τους ποιο σύνθετους τύπους **υψηλής αλληλεπίδρασης (high-interaction) honeypot**.

Συγκεκριμένα, είναι ένα υψηλής-αλληλεπίδρασης **honeypot** που προσπαθεί να παρέχει τη μέγιστη δυνατότητα αλληλεπίδρασης δίνοντας πραγματικά συστήματα για να αλληλεπιδρούν με αυτά οι επιτιθέμενοι, τίποτα δεν εξομοιώνεται. Πολλές φορές σχεδιάζονται ώστε να αντιγράφουν την πραγματικότητα, να παρέχουν δηλαδή ολοκληρωμένα αντίγραφα *δικτύων και* συστημάτων παραγωγής. Τα **Honeynets** είναι μια πολύ ισχυρή λύσης **honeypot**, ικανή να συλλέξει πληροφορίες που κανένα άλλο **honeypot** δεν μπορεί. Εντούτοις, είναι επίσης μια από τις πιο

σύνθετες λύσεις **honeypot**, που απαιτούν πολύ εργασία για την κατασκευή, συντήρηση και κυρίως την παρακολούθηση τους.

Ο στόχος ενός **honeynet**, είναι να συλλέγει δεδομένα (data) από κάθε δυνατή πηγή, ενώ ταυτόχρονα προστατεύει κάθε σύστημα παραγωγής, περιορίζοντας τις κακόβουλες κινήσεις του επιτιθέμενου εντός του **honeynet**. Η συλλογή των δεδομένων, υλοποιείται σε διαφορετικά επίπεδα , με σκοπό να καταγραφεί όσο γίνεται περισσότερη πληροφορία, χωρίς το γεγονός να γίνει αντιληπτό από τον επιτιθέμενο. Τα επίπεδα που συλλέγουμε την πληροφορία είναι τρία, στο πρώτο συλλέγουμε τα firewall logs, στο δεύτερο δεδομένα που παίρνουμε από το IDS (alerts, warnings , detections) και στο τρίτο επίπεδο τα δεδομένα από τα **honeypots.** Η πολυεπίπεδη συλλογή δεδομένων επιτρέπει την απόκτηση πλήρους εικόνας για τα δρώμενα εντός του **honeynet** και εξασφαλίζει έναν πλεονασμό πληροφορίας καλύπτοντας την περίπτωση αστοχίας κάποιου επιπέδου συλλογής δεδομένων. Το σύνολο των τεχνικών που υλοποιούνται για την συλλογή των δεδομένων αποκαλείται **Data Capture**.

Εκτός από τις αυξημένες δυνατότητες που παρέχει ένα **Honeynet** σε σύγκριση με τα **honeypots**, αντιμετωπίζει επίσης και αυξημένους κινδύνους. Όταν, το **honeynet** παραβιαστεί ο επιτιθέμενος μπορεί να χρησιμοποιήσει το **honeynet** για να επιτεθεί προς το παραγωγικό δίκτυο. Για να μετριαστεί αυτός ο κίνδυνος το **honeynet** εκτός από την δυνατότητα να συλλέγει data, υλοποιεί ελέγχους ώστε να μην γίνεται επικίνδυνο όταν θα παραβιαστεί. Ο στόχος είναι να περιορίζεται ο επιτιθέμενος ώστε να μην μπορεί να επιτεθεί σε συστήματα του παραγωγικού δικτύου και ταυτόχρονα να είναι ελεύθερος να κινηθεί προς και μέσα στο **Honeynet**. Επίσης η δράση των μηχανισμών που υλοποιούν τους ελέγχους πρέπει, να μην γίνει αντιληπτή από τον επιτιθέμενο. Το σύνολο των τεχνικών που υλοποιούνται για τον έλεγχο των δεδομένων ονομάζεται **Data Control.**

Στην συνέχεια θα δούμε, πώς υλοποιούμε ένα **honeynet** και ποια είναι η αξία του Data Capture και Data Control.

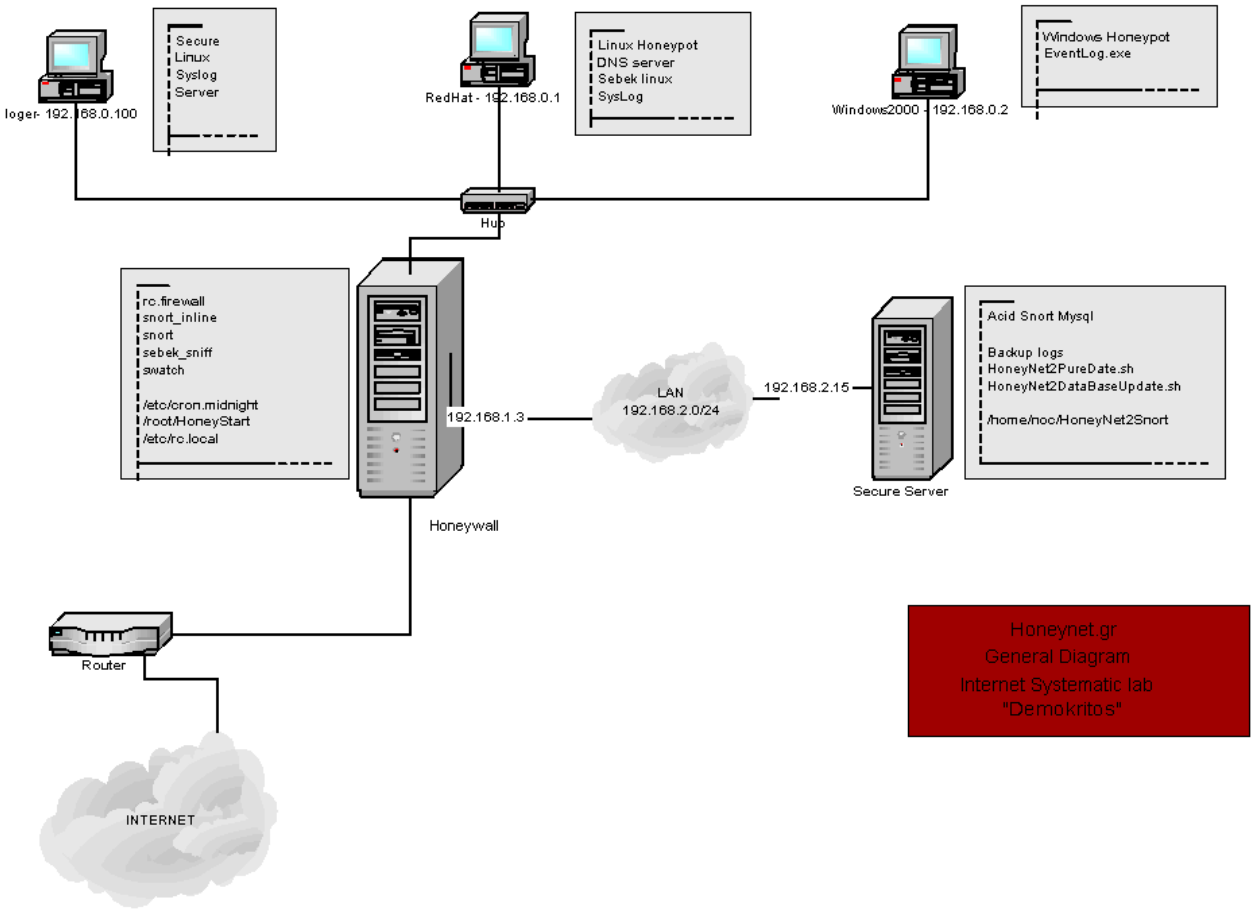
Αρχιτεκτονική και λειτουργία

Αρχιτεκτονική HoneyNet

Το **honeynet** δεν είναι ένα τυποποιημένο σύστημα. Η αρχιτεκτονική του, επιτρέπει να το διαμορφώνουμε σύμφωνα με τις απαιτήσεις μας. Ο σκοπός του **honeynet** είναι να δημιουργηθεί ένα ελεγχόμενο δίκτυο, ένα δίκτυο που να μπορεί να ελέγχει και να καταγράφει ότι δραστηριότητα γίνεται μέσα σ' αυτό. Μπορούμε να το παρομοιάσουμε σαν ένα ενυδρείο. Σε ένα ενυδρείο προσθέτουμε την άμμο, τα φύκια τα ψάρια και τα λοιπά, έτσι δημιουργείται ένα περιβάλλον στο οποίο μπορούμε να παρατηρούμε οτιδήποτε γίνεται μέσα σ' αυτό. Έτσι και στο **honeynet** δημιουργούμε ένα περιβάλλον αλλά αντί για ψάρια και κοράλλια έχουμε **βάσεις δεδομένων**, **web servers** , **DNS server** , ή ένα αρχείο μισθοδοσίας και γενικά συστήματα η αξία των οποίων, είναι το ότι αποτελούν στόχους επιθέσεων. Αυτή η διάταξη μας επιτρέπει να εντοπίζουμε και να συλλαμβάνουμε, εκτός από τα γνωστά **scans** και **exploits** , νέα εργαλεία και τακτικές επίθεσης. Ο εντοπισμός νέων εργαλείων και τακτικών καθώς και η αναγνώρισή τους δεν είναι εύκολα σε άλλες συνθήκες, αφού δεν υπάρχουν πληροφορίες για αυτά στις βάσεις πληροφοριών των συστημάτων εντοπισμού επιθέσεων (**IDS**). Σε αντίθεση με άλλα δίκτυα στο **Honeynet** δεν υπάρχει κίνηση που οφείλεται σε κανονική χρήση, οτιδήποτε αλληλεπιδρά με το **honeynet** είναι εξ' ορισμού ύποπτο.

Το βασικό στοιχείο της αρχιτεκτονικής του **honeynet** είναι η **πύλη-honeynet**, αποκαλούμενη **honeywall**. Ο σκοπός της πύλης ουσιαστικά είναι να διασύνδεει το honeynet με το παραγωγικό δίκτυο μας και το διαδίκτυο, αλλά και να το απομονώσει από αυτά. Τα διασύνδεει για να επιτρέψει τις επιθέσεις προς το **Honeynet** ενώ τα απομονώνει όταν υπάρχει ένδειξη ότι μια επίθεση ξεκινάει από το **Honeynet** προς άλλα δίκτυα ώστε να τα προστατέψει. Μπροστά από το **honeywall** είναι τα παραγωγικά συστήματα ενός οργανισμού και ότι υπάρχει πίσω από το **honeywall** είναι τα συστήματα στόχοι (**honeypots**). Τα **honeypots** είναι τα συστήματα με τα οποία αλληλεπιδρούν οι επιτιθέμενοι και το **honeywall** είναι αυτό που φροντίζει για την καταγραφή των δεδομένων (**data capture**) από και προς τα συστήματα "θύματα" αλλά και για τον έλεγχο και περιορισμό (**data control**) των επιθέσεων από τα συστήματα "θύματα" προς το παραγωγικό δίκτυο, έτσι ώστε να μικραίνει η πιθανότητα να επιτευχθεί επίθεση προς το παραγωγικό δίκτυο μέσω των **honeypots**.

Τοπολογία



Εικόνα 1-3 - Τοπολογία ενός honeynet.

Στην Εικόνα 1-3 Παρουσιάζεται ένα **honeynet**. Ξεκινώντας από το πάνω μέρος βλέπουμε τρία **honeypots**, τα οποία συνδέονται με ένα hub. Το hub επικοινωνεί και με το συστήματα που φαίνεται κάτω από τα **Honeypots** αριστερά, το οποίο είναι το **honeywall**. Δεξιά από το **honeywall** απεικονίζεται το δίκτυο διαχείρισης του **honeynet** και ο κεντρικός υπολογιστής που συγκεντρώνει τα δεδομένα από το **honeywall**. Στο κάτω μέρος τις εικόνας φαίνεται ο router που παρέχει την πρόσβαση στο internet.

Το **honeywall** χρησιμοποιείται για να χωρίζει τα **honeypots** από τα παραγωγικά συστήματα, επίσης να καταγράφει την κίνηση των **honeypots**, και μας δίνει την δυνατότητα να διαχειριζόμαστε αυτά τα δεδομένα.

Τα **honeypots**, στην συγκεκριμένη περίπτωση, επικοινωνούν μεταξύ τους και με το **honeywall** μέσο ενός **hub**. Δύο είναι τα πλήρως εκτεθειμένα συστήματα, το ένα έχει λειτουργικό σύστημα **Linux RedHat 7.2**, και το δεύτερο **honeypot** είναι ένα σύστημα με **Windows 2000 professional.** Και τα δύο μηχανήματα έχουν ενεργοποιημένα διάφορα ευπαθή services, όπως για παράδειγμα το service του ftp που επιτρέπει μεταφορά αρχείων από απομακρυσμένους χρήστες , με σκοπό να προσελκύσουν επιτιθέμενους. Το τρίτο είναι ο **Logger**, ένα σύστημα **Linux** που έχει σκοπό να καταγράφει γεγονότα συστήματος (**system logs**) από τα άλλα **honeynets**. Ο **Logger** είναι σχετικά ασφαλής διότι επιτρέπει πρόσβαση μόνο από μία πόρτα την οποία χρησιμοποιούν τα υπόλοιπα **honeypots** για να στέλνουν τα **logs** του συστήματος τους . Παρ' όλα αυτά δεν παύει να είναι και αυτό ένα **honeypot**, απλά ποιο ασφαλή από τα άλλα. Το να εντοπιστεί και να παραβιαστεί από έναν επιτιθέμενο, δεν είναι απώλεια για εμάς, αφού όλα όσα συμβαίνουν πίσω από το **honeywall** καταγράφονται, αντιθέτως θα έχουμε ανακαλύψει κάποια εξαιρετικά ενδιαφέρουσα μέθοδο και τεχνική καταγράφονται.

Το **Honeywall** έχει πολλαπλή χρησιμότητα. Κατ' αρχήν, λειτουργεί σαν **bridge (συσκευή OSI επιπέδου 2)** ανάμεσα στα **honeypots** και στο **δρομολογητή (router)** που παρέχει σύνδεση με το διαδίκτυο. Φυσικά ότι περνάει από το διαδίκτυο προς και από τα **honeypots**, καταγράφεται. Η σύλληψη των δεδομένων επιτυγχάνεται από το **IDS** που είναι εγκατεστημένο πάνω στο **honeywall** . Το **honeywall** επίσης χρησιμοποιείται ως **firewall** για να αποτρέπει τις τυχών επιθέσεις από κάποιο παραβιασμένο **honeypot** προς το υπόλοιπο δίκτυο ή προς το διαδίκτυο. Τέλος παρέχει δυνατότητα απομακρησμένης διαχείρισης του **Honeywall** δυνατότητα αποστολής των alerts μέσω e-mail, να επιτρέπει μεταφορά των δεδομένα που έχουν συλληφθεί σε άλλο σημείο για ανάλυση και λοιπάάλλες όμοιες λειτουργίες.

Η Λειτουργία Συλλογής Δεδομένων Του Honeynet

Data Capture

Η συλλογή δεδομένων αναφέρεται στην διαδικασία καταγραφής όλων των δραστηριοτήτων του επιτιθέμενου σε ένα **honeynet**. Είναι ένα σύνολο από τεχνικές που χρησιμοποιούνται με σκοπό να καταγραφεί όσο περισσότερη πληροφορία γίνεται χωρίς αυτό το γεγονός να γίνει αντιληπτό από τον επιτιθέμενο.

Η καταγραφή των δραστηριοτήτων πρέπει να υλοποιείται σε διαφορετικά επίπεδα , δεδομένου ότι με ένα επίπεδο δεν μπορούμε να συλλάβουμε όλα τα δεδομένα που χρειαζόμαστε. Για παράδειγμα αν συλλέγουμε μόνο τις πληκτρολογήσεις (**keystrokes**) που γίνονται στο **honeypot** και γίνει κάποιο download, ή εκτελεστεί και στην συνέχεια, διαγραφεί κάποιο εργαλείο, δεν θα έχουμε ιδέα τι εργαλείο ήταν αυτό και τι αλλαγές προκάλεσε στο σύστημά μας. Επίσης η αποθήκευση των δεδομένων δεν πρέπει να γίνεται τοπικά αλλά σε κάποιο απομακρυσμένο σύστημα, έτσι ώστε να μην γίνεται αντιληπτό από τον επιτιθέμενο. Χωρίς την αποτελεσματική συλλογή δεδομένων το **honeynet** δεν θα έχει καμία αξία διότι δεν θα υπάρχουν διαθέσιμα στοιχεία για ανάλυση της επίθεσης και των σχετικών γεγονότων.

Η Λειτουργία Ελέγχου Δεδομένων Του Honeynet

Data Control

Τα **honeynets** είναι ιδιαίτερά ευέλικτα περιβάλλοντα, επειδή δίνουν την δυνατότητα στον επιτιθέμενο να έχει την ελευθερία να κάνει ότι θέλει μέσα σε αυτά αφού τα παραβιάσει πρώτα. Αυτή η ελευθερία και η στενή παρακολούθηση όλων των κινήσεων του επιτιθέμενου και η καταγραφή όλης αυτής της πληροφορίας θα μας βοηθήσει να βγάλουμε πολύτιμα συμπεράσματα. Εκτός από τα θετικά στοιχεία, αυτής την ελευθερίας που δίνουμε στον επιτιθέμενο , υπάρχουν και κάποιοι αυξημένοι κίνδυνοι. Για παράδειγμα, ένας επιτιθέμενος μπορεί να επιτεθεί στο **honeynet**, να αποκτήσει τον έλεγχο κάποιου μηχανήματος, και να χρησιμοποιήσει αυτό το μηχάνημα για να εξαπολύσει κάποιο **exploit**, μία επίθεση άρνησης υπηρεσιών (**Denial Of Service Attack**) ή για διανομή **Warez** υλικού ή και για διανομή κλεμμένων αριθμών πιστωτικών καρτών.

Τα **honeynets** έχουν την δυνατότητα να προσφέρουν ελευθερία στον επιτιθέμενο και παράλληλα να εξασφαλίζουν ότι δεν μπορεί να βλάψει άλλα συστήματα. Για να το πετύχουμε αυτό πρέπει να εξασφαλίσουμε τον έλεγχο δεδομένων (**Data Control**).

Ο έλεγχος δεδομένων, είναι ένα σύνολο από μηχανισμούς που υλοποιούνται με σκοπό να περιορίσουν τον κίνδυνο που προκύπτει από την στιγμή που θα παραβιαστεί ένα σύστημα **honeypot** , ώστε να μην χρησιμοποιηθεί για επιθέσεις σε άλλα μη **honeypots** συστήματα. Η εφαρμογή του ελέγχου δεδομένων θα πρέπει να υλοποιηθεί με τέτοιο τρόπο ώστε να μην γίνεται αντιληπτό το γεγονός από τον επιτιθέμενο διότι θα υποψιαστεί ότι παρακολουθείται θα σβήσει τα ίχνη του πριν εξαφανιστεί.