ΚΕΦΑΛΑΙΟ 5
ΑΝΑΛΥΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΑ SNORT, ACID

Εισαγωγή

Στο κεφάλαιο αυτό θα γίνει παρουσίαση των αποτελεσμάτων που έβγαλε το snort. Το snort είναι ένα network intrusion detection system το οποίο παρακολουθεί την κίνηση σε ένα δίκτυο και παράγει alerts για οποιαδήποτε κακόβουλη κίνηση πιάσει, σύμφωνα με το σύνολο των κανόνων με το οποίο είναι ρυθμισμένο.

Το snort το οποίο χρησιμοποίησα υπήρχε ήδη εγκατεστημένο για το C-class του πειράματος, οπότε δεν χρειάστηκε να το στήσω από την αρχή. Ωστόσο, η εγκατάσταση και τροποποίηση του snort είναι μια σχετικά εύκολη δουλειά, που διευκολύνεται σε σημαντικό βαθμό από τον μεγάλο όγκο documentation και manual που βρίσκονται στο διαδίκτυο για αυτό [1]. Θέλουμε να επεξεργαστούμε τα δεδομένα των virtual hosts με το snort για να δούμε στοιχεία για συγκεκριμένες επιθέσεις, να δούμε ποιες επιθέσεις συμβαίνουν με μεγαλύτερη συχνότητα, ποια worms είναι ακόμα ενεργά και ποια όχι και να αναλύσουμε μερικές απο αυτές, για να μπορέσουμε να τις κατανοήσουμε.

Intrusion Detection Systems

Με δεδομένη την αύξηση των κακόβουλων ενεργιών και επιθέσεων στο διαδίκτυο, τα κλασσικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που περιέχουν αυτά και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις. Μία σχετικά νέα και συνεχώς αναπτυσσόμενη μέθοδος προστασίας, είναι η αυτοματοποιημένη *Ανίχνευση Επιθέσεων* (*Intrusion Detection*). Από τις διπλωματικές εργασίες “Μελέτη των επιθέσεων που στηρίζονται σε 1πακέτα με ψευδή IP διεύθυνση αποστολέα (IP spoofing)” του Ιωάννου Παπαπάνου [20] και “ISLAB HACK: Βασικές Έννοιες & Προγραμματισμός του SNORT 2.0” του Δημήτρη Πρίτσου [21] μαθαίνουμε τους παρακάτω ορισμούς που θα μας χρησιμεύσουν για την κατανόηση των θεμάτων σχετικά με τα IDS και το snort. Ο όρος Intrusion Detection σημαίνει ανίχνευση επιθέσεων και έχει να κάνει με την παρακολούθηση των γεγονότων που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο και την ανάλυσή τους για σημάδια επιθέσεων.

Ο όρος Intrusion Detection Systems (IDSs) σημαίνει συστήματα ανίχνευσης επιθέσεων και έχει να κάνει με software ή hardware προϊόντα, που αυτοματοποιούν την παραπάνω διαδικασία παρακολούθησης και ανάλυσης.

Η εξέλιξη των IDSs, είναι ραγδαία τα τελευταία χρόνια και συνεχώς γίνονται προσπάθειες για βελτίωσή τους, κυρίως στον τομέα των συμπτωμάτων από False Positives και False

Negatives που παρουσιάζουν. Τα false positives είναι οι λανθασμένες επισημάνσεις που παράγει ένα IDS, όταν ανιχνεύσει κάποιο γεγονός σαν περίπτωση πιθανής επίθεσης ενώ δεν είναι. Τα false positives είναι δυνατόν να προκύψουν από κακή ρύθμιση του IDS ή από περιπτώσεις γεγονότων που δεν μπορούν να διαχωριστούν σαφώς από μία επίθεση. 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.

Με την τρέχουσα μορφή τους τα IDSs παρέχουν σημαντική υποστήριξη στα ήδη υπάρχοντα μέτρα προστασίας ενός δικτύου και σε συνδυασμό με άλλους μηχανισμούς ασφάλειας, αποτελούν ένα σημαντικό εργαλείο για την παρακολούθηση και την αποτροπή δικτυακών επιθέσεων

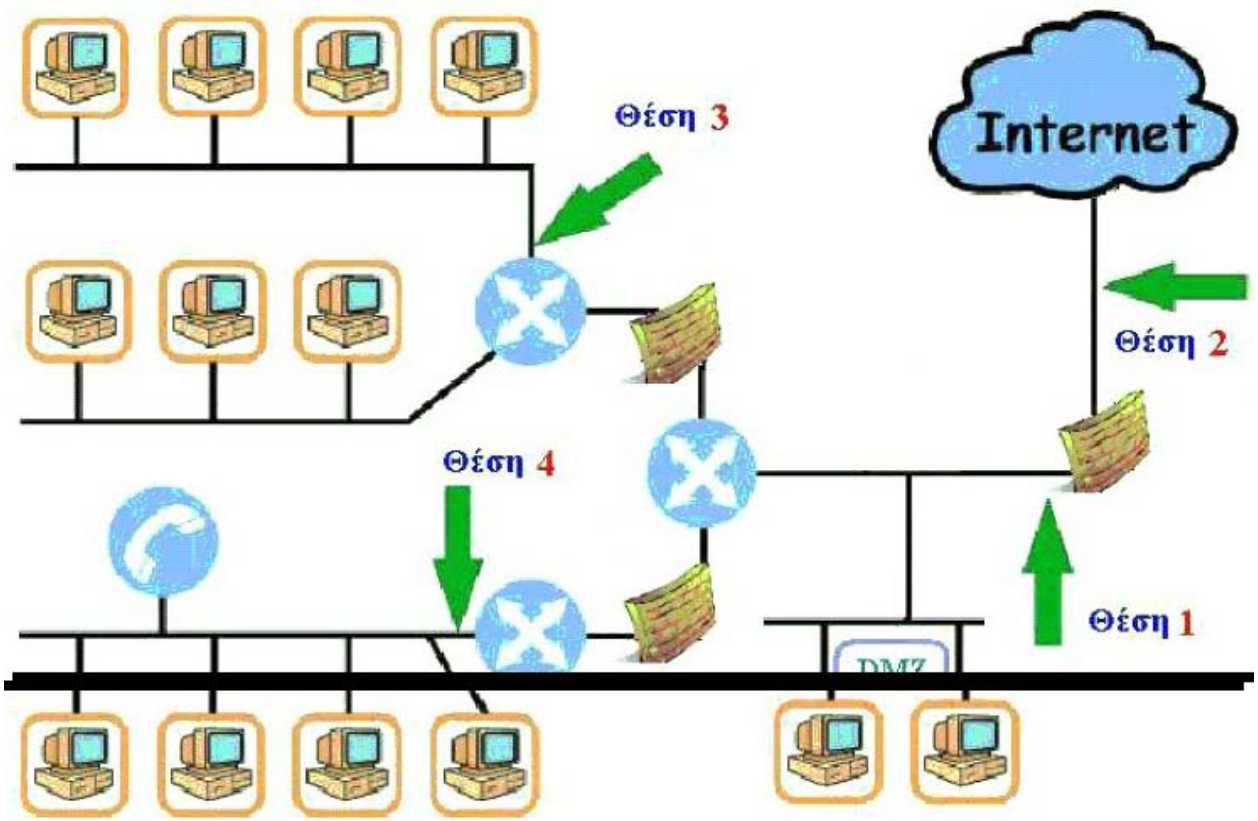
Alerts

Μία επισήμανση για την ανίχνευση κάποιας επίθεσης, συνήθως ονομάζεται *alert*. Τα περισσότερα IDSs δίνουν την δυνατότητα στον χρήστη να καθορίσει με σχετική ευχέρεια, την στιγμή και την μορφή που θα παράγονται τα *alerts* και σε ποιους χρήστες θα παρουσιάζονται. Ένα IDS είναι δυνατόν να ρυθμιστεί ώστε τα *alerts* να εμφανίζονται σε πραγματικό χρόνο, την ώρα που εντοπίζεται μία επίθεση, όπως για παράδειγμα με αναδυόμενα παράθυρα στην οθόνη ή μπορεί να ρυθμιστεί ώστε να καταγράφει τα *alerts* σε κάποιο αρχείο για μετέπειτα εξέταση, ή ακόμα και να τα στέλνει με email στον διαχειριστή του δικτύου.

Η μορφή που θα παράγεται ένα *alert* από το IDS, μπορεί να είναι από μία απλή αναφορά στο είδος της επίθεσης με έναν τίτλο, στον επιτιθέμενο και στο θύμα αυτής, μέχρι και αναλυτική αναφορά που θα περιέχει και πληροφορίες για το πακέτο που οδήγησε στον εντοπισμό της επίθεσης, κάνοντας λεπτομερή περιγραφή του ή αναφορά στο εργαλείο που χρησιμοποιήθηκε για την υλοποίησή της.

Τοποθέτηση του IDS

Η επιλογή του σημείου στο δίκτυο που θα τοποθετηθεί το IDS πρέπει να γίνει αφού ληφθούν υπόψιν διάφορα κριτήρια, αφού θα καθορίσει τη φύση των αποτελεσμάτων που θέλουμε να πάρουμε απο το IDS. Έχει διαφορά πχ αν το IDS τοποθετηθεί πίσω απο το firewall ή μπροστά, ή αν θα παρακολουθεί μόνο ένα συγκεκριμένο υποδίκτυο. Οι παρακάτω θέσεις είναι πιθανές για την τοποθέτηση του IDS:



Εικόνα 5.1-θέσεις τοποθέτησης ενός IDS

Το snort

Το Snort είναι ένα ΄lightweight΄ Network Intrusion Detection System (NIDS), καθώς και ένα εργαλείο ανάλυσης πακέτων το οποίο στηρίζεται στην βιβλιοθήκη libpcap. Ο δημιουργός του Snort είναι ο Martin Roesch ο οποίος ξεκίνησε την ανάπτυξη του κώδικά σε γλώσσα προγραμματισμού C, ενώ σήμερα ένας μεγάλος αριθμός ατόμων έχει εμπλακεί σε αυτήν την διαδικασία, με στόχο την προσθήκη νέων λειτουργιών στο Snort και την βελτίωση των δυνατοτήτων του. Σημαντικό ρόλο για το γεγονός αυτό παίζει ότι το Snort είναι ένα Open Source λογισμικό, το οποίο διατίθεται κάτω από την GNU General Public License (GPL) που καθιστά ελεύθερη την χρήση και ανάπτυξη του κώδικά του από τον καθένα. Ο όρος ΄lightweight΄ έχει δύο έννοιες. Η μία έχει να κάνει με την εφαρμογή του σε σχετικά μικρά δίκτυα, ενώ η δεύτερη έχει να κάνει με το μικρό μέγεθος του και την ευκολία εφαρμογής και χρήσης του.

Το Snort εκτός από την λειτουργία του σαν NIDS μπορεί να δουλέψει και σαν ένας απλός sniffer ή σαν ένας sniffer που καταγράφει(logging) τα πακέτα που λαμβάνει σε log αρχεία σε μορφή απλού κειμένου ASCII. Έχει τρία mode λειτουργίας :

1 Sniffer mode.
2 Packet logger mode.
3 NIDS mode.

Sniffer Mode

Σε αυτό το mode λειτουργίας το Snort έχει την ικανότητα να διαβάζει τα πακέτα που περνάνε από το δίκτυο, να τα αποκωδικοποιεί και να τα εμφανίζει στην οθόνη σε φιλική προς τον χρήστη μορφή.

Packet Logger Mode

Σε αυτό το mode λειτουργίας το Snort αποθηκεύει στο δίσκο τα πακέτα που διαβάζει από το δίκτυο, αντί απλά να τα εμφανίζει στην οθόνη. Η διαδικασία αυτή είναι αρκετά σημαντική στην περίπτωση που απαιτείται τα πακέτα αυτά να εξεταστούν με λεπτομέρεια σε επόμενο στάδιο. Το Snort μπορεί να αποθηκεύσει τα πακέτα αυτά σε διάφορα formats, ανάλογα με τις ανάγκες του χρήστη, για παράδειγμα μπορεί να αποθηκεύσει τα πακέτα σε binary μορφή (tcpdump format), με την οποία μπορούν να χρησιμοποιηθούν σαν είσοδο σε διάφορα άλλα προγράμματα ανάλυσης πακέτων και πρωτοκόλλων, σε ASCII μορφή ώστε να είναι δυνατή η ανάγνωσή τους, σε XML μορφή ή και να οργανωθούν σε βάσεις δεδομένων.

NIDS Mode

Αυτή είναι η κύρια λειτουργία του Snort. Όπως αναφέρθηκε προηγουμένως, το Snort είναι ένα IDS το οποίο ενεργεί σε επίπεδο δικτύου, δηλαδή τα γεγονότα που παρακολουθεί και εξετάζει για την εμφάνιση μίας πιθανής επίθεσης, αφορούν την δραστηριότητα που παρατηρείται σε ένα δίκτυο. Το Snort έχει την ικανότητα να ανιχνεύει ένα μεγάλο φάσμα από γνωστές δικτυακές επιθέσεις, όπως *portscans, buffer overflows, OS fingerprints* και πολλά άλλα. Η τεχνική που χρησιμοποιεί το Snort για την διαδικασία αυτή είναι κατά κύριο λόγο η *Misuse Detection* με την χρήση των *Signatures* ενός βλαβερού(malicious) πακέτου. Το snort όμως ειδικά μετά την έκδοση 2.0 συνδυάζει στην λειτουργία της ανάλυσης των γεγονότων για την ανίχνευση πιθανών επιθέσεων και κάποιες από τις μεθόδους του *Protocol Anomaly Detection* και του *Anomaly Detection*. Οι μηχανισμοί αυτοί υλοποιούνται κατά κύριο λόγο από τους preprocessors αλλά και από το νέο μηχανισμό του snort 2.0 να συντάσσει τα rules σε κατηγορίες.

snort signatures και alerts

Το snort χρησιμοποιεί αρχεία με υπογραφές που ταιριάζουν κάποια χαρακτηριστικά μιας συγκεκριμένης επικοινωνίας. Τα *Signatures* του Snort ονομάζονται και *Rules,* καθώς είναι κανόνες οι οποίοι περιγράφουν τα χαρακτηριστικά ενός πακέτου που μπορεί να είναι μέρος μίας γνωστής επίθεσης, καθώς και την ενέργεια που θα εκτελεστεί κατά τον εντοπισμό του. Κάθε πακέτο που εντοπίζεται από το Snort, ελέγχεται για το αν έχει τα ίδια χαρακτηριστικά με αυτά που περιγράφονται από κάποιο *Rule*. Τα *Rules* του Snort μπορούν να γραφτούν σε

απλή περιγραφική γλώσσα σε ASCII μορφή και κάθε ένα από αυτά αποτελείται από δύο λογικά μέρη, τον *Rule Header* και τα *Rule Options*.

Παράδειγμα υπογραφής του snort είναι το εξής:

alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR subseven 22";flow:to_server,established; content:"|0d0a5b52504c5d3030320d0a|";reference:arachnids,485; reference:url, www.hackfix.org/subseven/; classtype:misc-activity; sid:103; rev:5;)

Ο κανόνας αυτός θα δημιουργήσει ένα alert όταν εντοπίσει το backdoor subseven. Η υπογραφή ταιριάζει τα πακέτα που περιέχουν το string 0d0a5b52504c5d3030320d0a, το οποίο είναι χαρακτηριστικό του subseven.

Ο επόμενος κανόνας εντοπίζει το buffer overflow στον iis με webdav που ανακαλύφθηκε το 2003:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS WEBDAV exploit attempt"; flow:to_server,established; content:"HTTP/1.1|0a|Content-type|3a| text/xml|0a|HOST|3a|"; content:"Accept|3a| |2a|/|2a0a|Translate|3a| f|0a|Contentlength| 3a| 5276|0a0a|"; distance:1; reference:cve,CAN-2003-0109; reference:bugtraq,7716; classtype:attempted-admin; sid:2090; rev:2;)

Ανάλυση και ταίριασμα υπογραφών εκτός από το snort κάνουν και τα υπόλοιπα intrusion detection συστήματα, αλλά ακόμα και το iptables [2], το πολύ διάσημο open source packet filter/firewall.

Το Snort διανέμεται με πάνω από 2500 έτοιμα *Signatures,* για χρήση τους στην ανίχνευση γνωστών επιθέσεων, ενώ για την δημιουργία νέων *Rules* προσφέρει μία μεγάλη γκάμα από options που μπορεί ο χρήστης να χρησιμοποιήσει, τα οποία του δίνουν την ευελιξία να εκτελεί λεπτομερής και σε βάθος περιγραφή των χαρακτηριστικών του κάθε πακέτου, για το οποίο θέλει να γίνει έλεγχος για τον εντοπισμό μίας επίθεσης. Επίσης υπάρχει και το site bleeding snort rules [18] στο οποίο δημοσιεύονται πειραματικά rules, τα οποία μετά από λίγο καιρό ενσωματώνονται σαν επίσημα rules για το snort. Όταν το Snort ανιχνεύσει μία επίθεση έχει την δυνατότητα να γνωστοποιήσει τα αποτελέσματά του με διάφορους τρόπους, με την μορφή *alerts*. Κάποιοι από αυτούς είναι, σε πραγματικό χρόνο με την χρήση αναδυόμενων παραθύρων στην οθόνη, σε ASCII μορφή στην κονσόλα, να τα αποθηκεύσει σε αρχεία σε ASCII μορφή για μετέπειτα ανάγνωση ή και να τα οργανώσει σε βάσεις δεδομένων όπως MySQL, PostgreSQL,Oracle, unixODBC, κ.α. Ένα alert μπορεί να δώσει πληροφορίες για μια

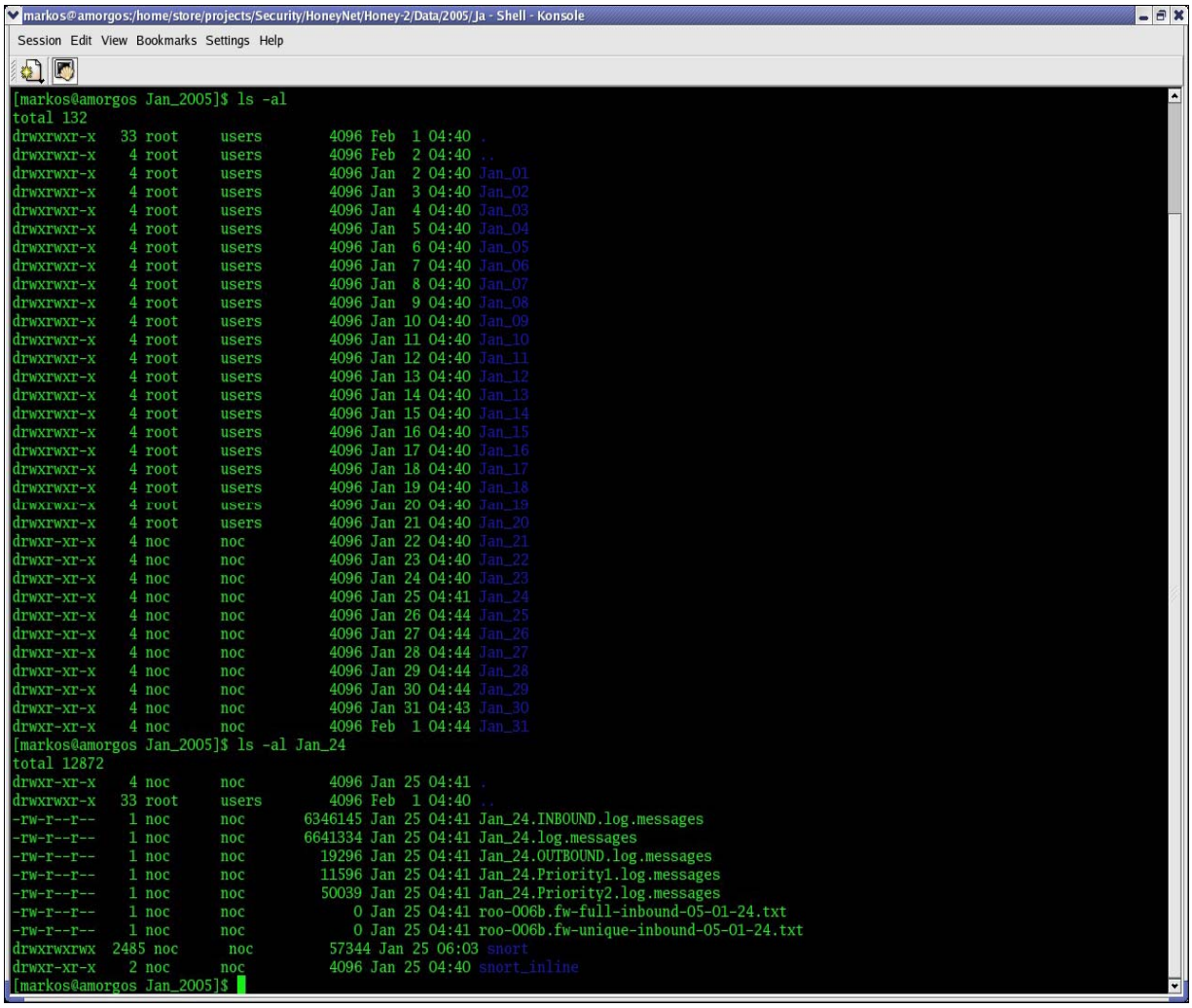
επίθεση, όπως το είδος της, τον επιτιθέμενο και το στόχο, αν είναι υψηλής προτεραιότητας ή όχι και φυσικά ποια πακέτα οδήγησαν στην ανίχνευση της επίθεσης.

Στο παρακάτω σχήμα παρουσιάζεται ένα *alert* του Snort.

[**] [1:553:4] POLICY FTP anonymous login attempt [**] [Classification: Misc activity] [Priority: 3] 03/11-12:23:37.280737 192.168.0.9:1245 -> 192.168.100.25:21 TCP TTL:128 TOS:0x0 ID:13318 IpLen:20 DgmLen:56 DF ***AP*** Seq: 0x74603DEF Ack: 0x7B16BDCC Win: 0xFAB2 TcpLen: 20

Το *alert* αυτό δημιουργήθηκε από το Snort καθώς εντόπισε μία προσπάθεια για σύνδεση ενός χρήστη σαν anonymous, στον ftp server με την IP διεύθυνση 192.168.100.25. Κάποιοι ftp servers επιτρέπουν την χρήση τους από χρήστες που δεν έχουν έναν εξουσιοδοτημένο λογαριασμό, αν αυτοί συνδεθούν με το username anonymous και δώσουν για password την mail διεύθυνσή τους. Αυτό όμως μπορεί να δημιουργήσει τρύπες ασφάλειας σε έναν ftp server και για αυτό κάποιοι δεν επιτρέπουν την χρήση του κοινού λογαριασμού anonymous. Στην περίπτωση που ο συγκεκριμένος ftp server δεν επιτρέπει σε χρήστες χωρίς κάποιο εξουσιοδοτημένο προσωπικό λογαριασμό να συνδεθούν σε αυτόν, τότε αυτό το *alert* μπορεί να είναι μία ένδειξη για προσπάθεια παραβίασης του συστήματος. Στο δείγμα του *alert* που παρουσιάζεται αναφέρεται η ώρα που ανιχνεύτηκε το γεγονός καθώς και το είδος της επίθεσης που εντοπίστηκε, ενώ ακολουθεί περιγραφή των χαρακτηριστικών του πακέτου που οδήγησε στην δημιουργία του *alert*.

Καταγραφή γεγονότων (Logging)



Εικόνα 5.2-logs του snort

Το snort δημιουργεί έναν φάκελο για κάθε μέρα λειτουργίας του, μέσα στον οποίο δημιουργεί τα εξής αρχεία:

- **Μήνας_Μέρα.log.messages**
  Όπως τα logs από ένα firewall, στο αρχείο αυτό καταγράφει στοιχεία όπως source/destination hosts και ports για όλες τις εισερχόμενες και εξερχόμενες συνδέσεις.
- **Μήνας_Μέρα.INBOUND.log.messages**
  Όπως το log.messages αλλά μόνο για τις εισερχόμενες συνδέσεις.
- **Μήνας_Μέρα.OUTBOUND.log.messages**
  Όπως το log.messages αλλά μόνο για τις εξερχόμενες συνδέσεις.
- **Μήνας_Μέρα.Priority1.log.messages**
  Καταγράφει τα πιο σοβαρά alerts που εντόπισε σε μορφή για γρήγορη ανάλυση.

- **Μήνας_Μέρα.Priority2.log.messages**
  Καταγράφει τα λιγότερο σοβαρά alerts -priority2.
- **snort/snort_full**
  Στο αρχείο αυτό καταγράφονται όλα τα alerts που εντόπισε το snort, με κάποιες πληροφορίες και συχνά links για το συγκεκριμένο vulnerability από κάποιο μεγάλο site σχετικό με την ασφάλεια δικτύων.
- **snort/snort_fast**
  Όπως και το προηγούμενο αρχείο, σε όχι τόσο αναλυτική μορφή.
- **snort/pcap.xxxxxxxxxxxxxxxxxxxxx**
  Στο αρχείο αυτό αποθηκεύεται ολόκληρη η κίνηση -εισερχόμενη και εξερχόμενη-σε δυαδική μορφή -binary-ώστε να μπορεί να επεξεργαστεί με το tcpdump ή ethereal.
- **snort/portscan.log**
  Καταγράφει τα port scannings που έγιναν.

Αρχείο μήνας_Μέρα.log.messages

markos@amorgos$ more Jan_24.INBOUND.log.messages

...

Jan 24 13:35:56 bilem3 kernel: INBOUND UDP: IN=br0 PHYSIN=eth2 OUT=br0 PHYSOUT=eth1 SRC=12.232.107.41 DST=143.xxx.xxx.178 LEN=908 TOS=0x00 PREC=0x80 TTL=109 ID=26040 PROTO=UDP SPT=22604 DPT=1027 LEN=888

Jan 24 13:35:56 bilem3 kernel: INBOUND UDP: IN=br0 PHYSIN=eth2 OUT=br0 PHYSOUT=eth1 SRC=12.105.119.97 DST=143.xxx.xxx.177 LEN=908 TOS=0x00 PREC=0x80 TTL=108 ID=26040 PROTO=UDP SPT=18386 DPT=1027 LEN=888

Jan 24 13:35:56 bilem3 kernel: INBOUND UDP: IN=br0 PHYSIN=eth2 OUT=br0 PHYSOUT=eth1 SRC=12.98.64.117 DST=143.xxx.xxx.183 LEN=908 TOS=0x00 PREC=0x80 TTL=109 ID=29880 PROTO=UDP SPT=28275 DPT=1027 LEN=888

Εδώ καταγράφονται οι νέες εισερχόμενες και εξερχόμενες συνδέσεις. Ακολουθεί η ανάλυση της δομής μιας καταγραφής στο αρχείο:

πεδίο	***πρωτόκολλο***	***σχόλια***
Jan 24 13:35:56	ip	Ημερομηνία και ώρα

πεδίο	***πρωτόκολλο***	***σχόλια***
bilem3	ip	Το hostname του snort host
INBOUND UDP	ip	Η σύνδεση είναι εισερχόμενη udp

IN=br0 PHYSIN=eth2	ip	Το πακέτο εισήλθε από το interface eth2 του bilem3
OUT=br0 PHYSOUT=eth1	ip	Το πακέτο έφυγε από το eth1
SRC=12.98.64.117	ip	Η ip του source host
DST=143.xxx.xxx.183	ip	Η ip του destination host
LEN=908	ip	Το μέγεθος του πακέτου
TOS=0x00	ip	Type of service
PREC=0x80	ip	Προτεραιότητα του πακέτου
TTL=109	ip	Time to live
ID=29880	ip	Αριθμός αναγνώρισης του πακέτου
PROTO=UDP	ip	Το transport layer είναι το udp
SPT=28275	udp	Η source port
DPT=1027	udp	Η destination port

αρχείο snort/snort_full

markos@amorgos$ more snort/snort_full ...
[1]
[**] [1:2314:1] SHELLCODE x86 0x90 NOOP unicode [**]
[Classification: Executable code was detected] [Priority: 1]
01/24-15:05:39.804380 143.xxx.xxx.55:2450 -> 143.xxx.xxx.94:445
TCP TTL:127 TOS:0x0 ID:41832 IpLen:20 DgmLen:1500 DF
AP Seq: 0x7DD467A Ack: 0xC6AF6770 Win: 0x4470 TcpLen: 32
TCP Options (3) => NOP NOP TS: 255070 2021548

[2]
[**] [1:1042:6] WEB-IIS view source via translate header [**]
[Classification: access to a potentially vulnerable web application] [Priority: 2] 01/24-15:14:31.361567 143.xxx.xxx.86:4193 -> 143.xxx.xxx.94:80 TCP TTL:127 TOS:0x0 ID:59583 IpLen:20 DgmLen:202 DF ***AP*** Seq: 0x9E7985F9 Ack: 0xC70467E2 Win: 0xFAF0 TcpLen: 32 TCP Options (3) => NOP NOP TS: 109206 2022635 [Xref => http://www.securityfocus.com/bid/1578][Xref => http://www.whitehats.com/info/IDS305]

[3]

[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/24-18:53:08.265874 213.148.225.230 -> 143.xxx.xxx.32
ICMP TTL:112 TOS:0x80 ID:58783 IpLen:20 DgmLen:28
Type:8 Code:0 ID:512 Seq:23140 ECHO
[Xref => http://www.whitehats.com/info/IDS162]

Στην πρώτη περίπτωση είναι ένα alert που έχει παράγει το snort με priority1, δηλαδή πρόκειται για κάποιο σοβαρό alert. Ο 143.xxx.xxx.251.55 επιχείρησε να τρέξει κάποιο exploit προς τον 143.xxx.xxx.94 στην πόρτα 445, πιθανώς πρόκειται για κάποιο worm. Αν το snort που τρέχουμε ήταν ενημερωμένο όσον αφορά τα τελευταία worms, θα έβγαζε το alert οτι έγινε προσπάθεια μετάδοσης για το συγκεκριμένο worm, αντί για το “SHELLCODE x86 0x90 NOOP unicode” που βγάζει όταν εντοπίζει κακόβουλο κώδικα αλλά δεν μπορεί να τον προσδιορίσει.

Στην δεύτερη περίπτωση το snort έχει εντοπίσει την επίθεση που έγινε και μάλιστα μας δίνει και links για να βρούμε πληροφορίες.

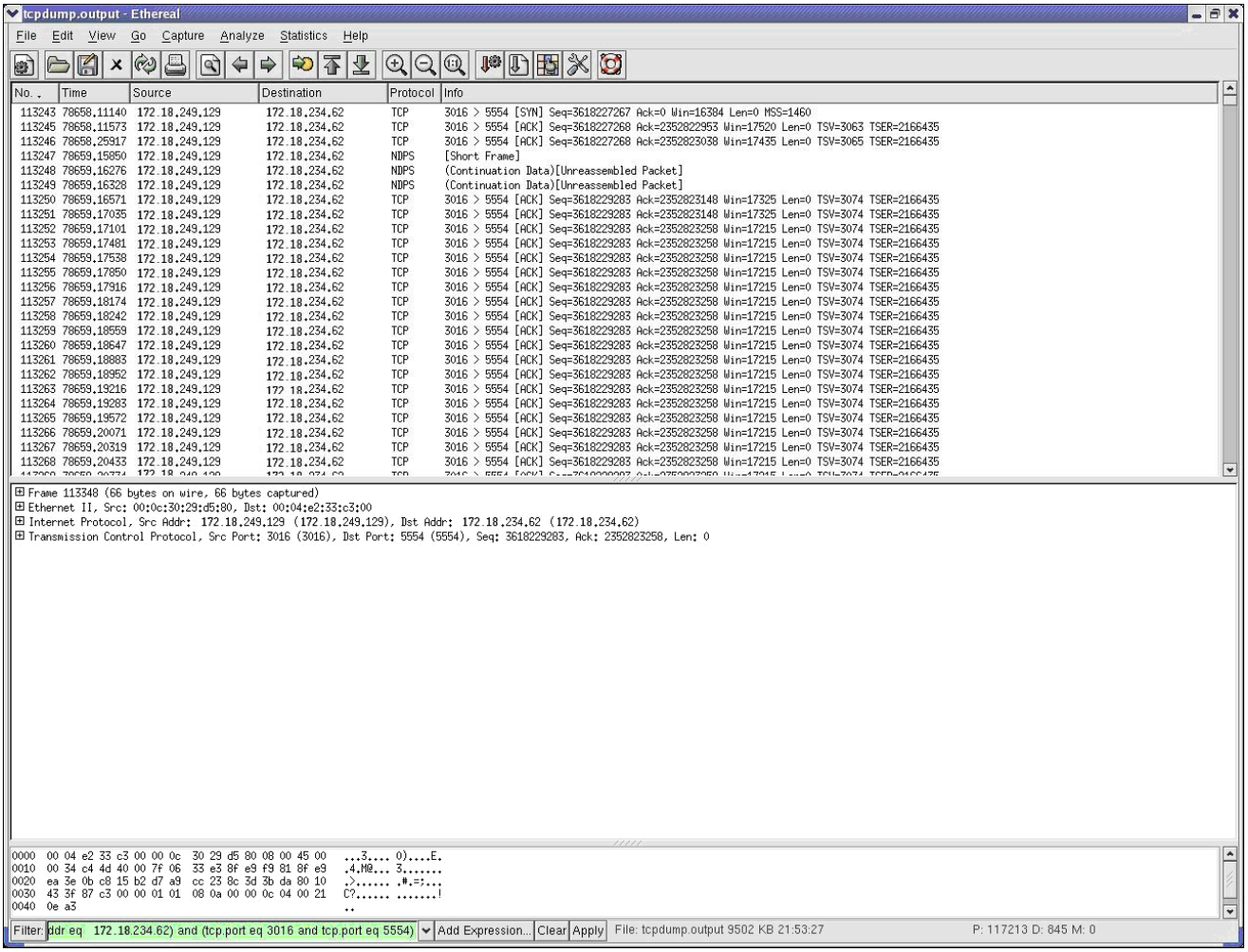
Το securityfocus.com είναι από τα πιο διάσημα sites στον τομέα της ασφάλειας δικτύων και μπορεί κανείς να βρει οτιδήποτε σχετικό. Μεταξύ άλλων περιέχει πλήθος από άρθρα, μελέτες, αναλύσεις και case studies, τα τελευταία νέα και εξελίξεις από τον χώρο της ασφάλειας δικτύων και forums συζητήσεων. Μια απο τις πιο ενδιαφέρουσες υπηρεσίες που προσφέρει το securityfocus είναι το ότι διαθέτει την πιο ενημερωμένη και ολοκληρωμένη βάση δεδομένων με vulnerabilities που υπάρχει στο internet. Η βάση αυτή περιλαμβάνει πληροφορίες για τα vulnerabilities, τον τρόπο που λειτουργούν, ποιες υπηρεσίες και λειτουργικά συστήματα αναλυτικά επηρεάζουν και πως μπορούν να αντιμετωπιστούν. Στις περισσότερες φορές μάλιστα υπάρχει και ο κακόβουλος κώδικας ώστε να μπορεί να διαπιστώσει κάποιος αν το σύστημα του είναι ευάλωτο στο συγκεκριμένο vulnerability. Το securityfocus.com είναι το ιδανικό μέρος για να ξεκινήσει κάποιος αρχάριος να μαθαίνει για την ασφάλεια δικτύων, μέχρι τους επαγγελματίες ερευνητές για να βρουν τις πληροφορίες που θέλουν.

Εικόνα 5.3-το site securityfocus.com

snort/pcap.xxxxxxxxxxxxxxxxxxxxx

Η επεξεργασία του αρχείου με τη δικτυακή κίνηση γίνεται με το ethereal [3], σε γραφικό περιβάλλον. Φορτώνουμε το αρχείο στο ethereal και από κει και πέρα μπορούμε ψάξουμε για συγκεκριμένες συνδέσεις και να τις δούμε ολόκληρες.

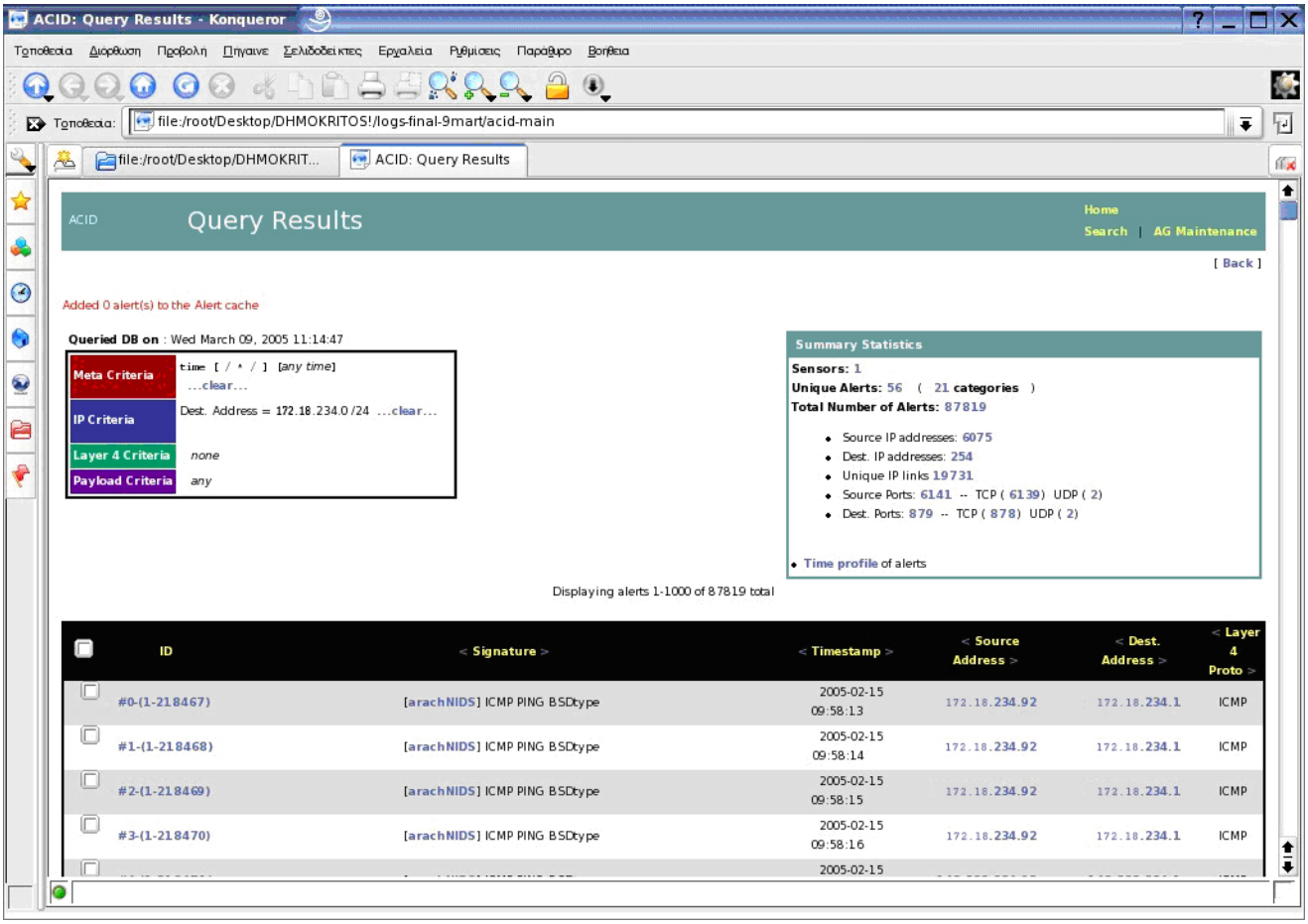
Αρχείο με τη δικτυακή κίνηση μπορούμε επίσης να δημιουργήσουμε με το να τρέχουμε το tcpdump στον honeyd host μας.



Εικόνα 5.4-επεξεργασία αρχείου δικτυακής κίνησης με το ethereal

ACID

Το acid[4] είναι ένα ισχυρό εργαλείο ανάλυσης δεδομένων γραμμένο σε php, για περιστατικά ασφάλειας καταγραμμένα από διάφορα IDS συστήματα, όπως τα snort, tcpdump.Το acid είναι το πιο εύχρηστο από τα front-ends που κυκλοφορούν για την επεξεργασία των αρχείων του snort και την ευκολότερη ανάλυση των δεδομένων. Είναι ιδιαίτερα χρήσιμο , καθώς μπορεί να πραγματοποιήσει αναζήτηση με βάση διάφορα κριτήρια, όπως κάποιο συγκεκριμένο alert, host, destination port, source address, ημερομηνία κ.α.



Εικόνα 5.5-το περιβάλλον του acid

Σαν κριτήρια αναζήτησης δίνουμε στο acid να ψάχνει -στα logs του snort-για -14 destination address ολόκληρο το C-class με τα virtual hosts μας. Το acid μας επιστρέφει οτι υπάρχουν συνολικά 87819 alerts για το παραπάνω adress space, ενώ τα unique alerts είναι 56. Αν το snort μας έτρεχε με πιο ανανεωμένους κανόνες, τότε πιθανόν θα έβρισκε περισσότερα unique alerts. Πχ πολλές απο τις απόπειρες worms για εξάπλωση απλά τις κατηγοριοποίησε στο alert “SHELLCODE EXECUTION”.

Τονίζεται στο σημείο αυτό για μια ακόμη φορά οτι το snort καταγράφει μόνο τα alerts που μπορεί να δημιουργήσει και όχι όλη την κίνηση. Πχ μια σύνδεση στην πόρτα 80 όπου απλά θα εκτελεί κάποιος την εντολή “HEADERS / HTTP/1.0 “ προσπαθώντας να δει ποιον web server χρησιμοποιούμε και τι έκδοση, ώστε να συγκεντρώσει όσο περισσότερα στοιχεία για να επιτεθεί, αν και πρόκειται για κακόβουλη ενέργεια για τα virtual hosts μας, το snort δεν θα την καταγράψει σαν alert. Με το snort μπορούμε να δούμε ποιες επιθέσεις συμβαίνουν στο δίκτυο μας, ποιους hosts επηρέασαν και να καταλάβουμε αν παραβιάστηκαν.

Το acid μας ενημερώνει ότι δημιούργησε alerts για 6075 διαφορετικά ip's, ενώ τα destination ports ήταν 879. Βέβαια στο προηγούμενο κεφάλαιο είδαμε οτι 187.403 διαφορετικές ip's επικοινώνησαν με τα virtual hosts μας. Η μεγάλη αυτή διαφορά εξηγείται ακριβώς επειδή το snort παράγει alerts μόνο όταν εντοπίσει μια προσπάθεια για διείσδυση με βάση τους κανόνες που έχει.
Τα alerts παρουσιάζονται με την μορφή:

ID #35-(1-232470)
Το νούμερο του alert.

<Signature> [url] [CVE] [bugtraq] [arachNIDS]WEB-FRONTPAGE rad fp30reg.dll access
Η ονομασία του alert -τις περισσότερες φορές το snort δίνει και κάποιο link ώστε να βρίσκουμε απευθείας πληροφορίες για το συγκεκριμένο vulnerability. Τα links είναι από κάποιο από τα: securityfocus.com, whitehats.com, cve.mitre.org.

<Timestamp> 2005-02-19 04:38:56
Η ημερομηνία και ώρα δημιουργίας του alert.

<Source Address> 64.213.188.94:42396
Η ip του host που δημιούργησε το alert.

<Dest.Address> 192.168.0.2:80
Η ip του host στον οποίο απευθύνοταν η source address.

<Layer 4 Proto> TCP
Το πρωτόκολλο -tcp, udp ή icmp.

Έχει μεγάλο ενδιαφέρον να δούμε ποια ήταν τα unique alerts που έβγαλε το snort

και σε τι συχνότητα το καθένα. Ο παρακάτω πίνακας περιέχει τα unique alerts.

ALERTS	***ΕΜΦΑΝΙΣΗ***
ICMP PING	32158
WEB-IIS view source via translate header	13988
TCP CHECKSUM CHANGED ON RETRANSMISSION (possible fragroute) detection	8064
SHELLCODE x86 unicode NOOP	8030
SHELLCODE x86 NOOP	6006
ICMP PING NMAP	5911
WEB-FRONTPAGE rad fp30reg.dll access	3487
WEB-MISC webdav search access	2409
possible EVASIVE RST detection	2622
ICMP Destination Unreachable (Communication Administratively Prohibited)	1692
ICMP PING CyberKit 2.2 Windows	535
TCP TOO FAST RETRANSMISSION WITH DIFFERENT DATA SIZE (possible fragroute) detection	449
SCAN SOCKS Proxy attempt	302

ALERTS	***ΕΜΦΑΝΙΣΗ***
WEB-IIS cmd.exe access	294
ICMP PING BSDtype	274
ICMP PING Delphi-Piette Windows	254
WEB-IIS ISAPI .ida attempt	191
SCAN Squid Proxy attempt	146
ICMP PING Windows	102
ICMP Echo Reply	96

ICMP Destination Unreachable (Undefined Code!)	87
ICMP Time-To-Live Exceeded in Transit	74
WEB-IIS multiple decode attempt	64
ICMP PING Sun Solaris	62
DNS zone transfer TCP	58
SCAN Proxy (8080) attempt	52
WEB-IIS CodeRed v2 root.exe access	38
ICMP Destination Unreachable (Port Unreachable)	35
WEB-IIS unicode directory traversal attempt	34
WEB-IIS unicode directory traversal attempt	29
SNMP trap tcp	27
STEALTH ACTIVITY (unknown) detection	25
WEB-FRONTPAGE /_vti_bin/ access	24
SNMP request tcp	24
ICMP Destination Unreachable (Host Unreachable)	20

ALERTS	***ΕΜΦΑΝΙΣΗ***
WEB-IIS unicode directory traversal attempt	18
WEB-IIS unicode directory traversal attempt	17
WEB-IIS _mem_bin access	17
SCAN nmap TCP	16
STEALTH ACTIVITY (NULL scan) detection	12
ICMP Fragment Reassembly Time Exceeded	9

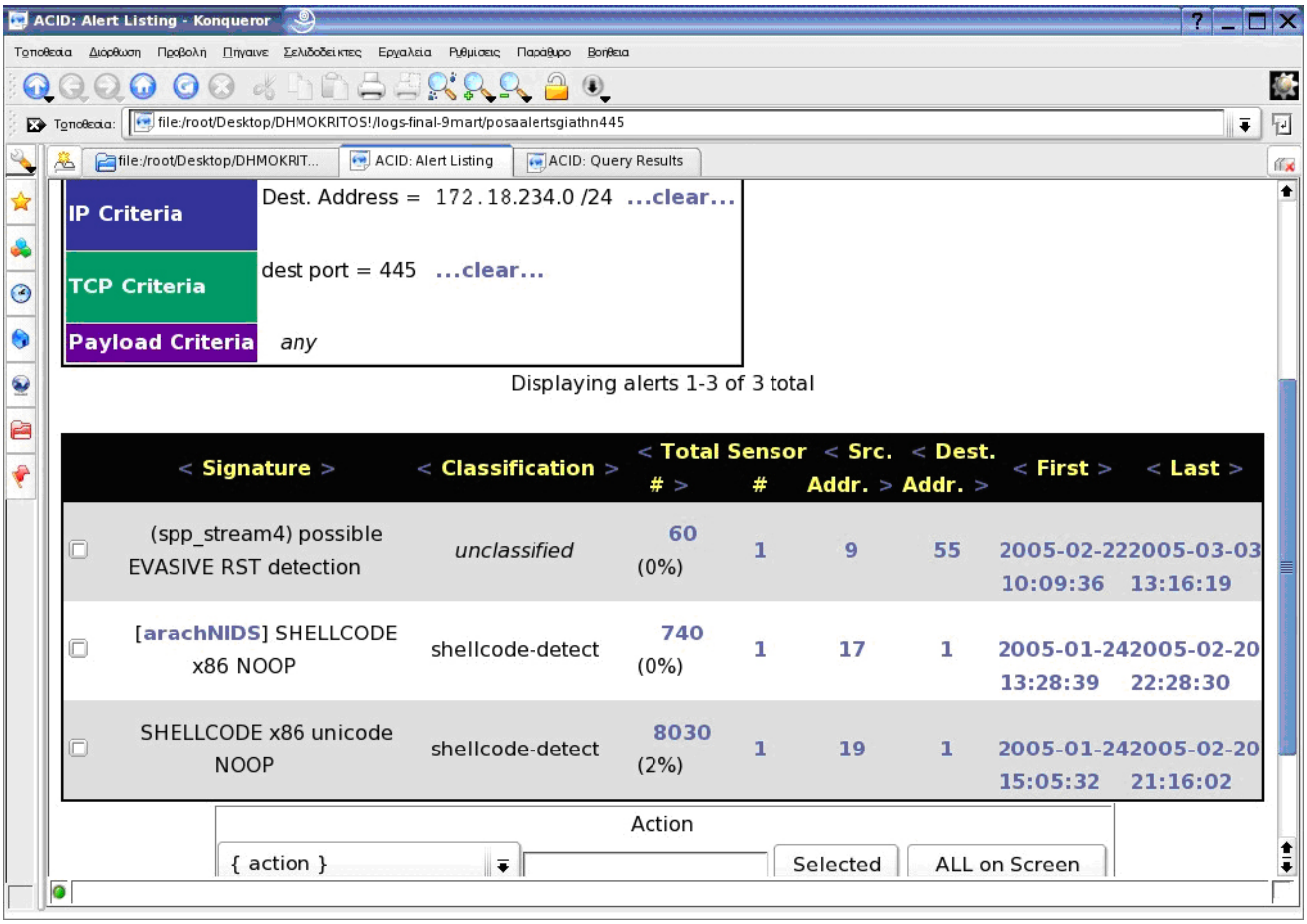
(spp_stream4) STEALTH ACTIVITY (XMAS scan) detection	8
(snort_decoder) WARNING: TCP Data Offset is less than 5!	6
RPC portmap listing TCP 111	5
WEB-MISC whisker space splice attack	4
Truncated Tcp Options	3
POLICY FTP anonymous login attempt	3
ICMP Source Quench	2
Tcp Options found with bad lengths	1
ICMP Destination Unreachable (Network Unreachable)	1
BAD TRAFFIC tcp port 0 traffic	1
DDOS mstream client to handler	1
WEB-IIS Unicode2.pl script (File permission canonicalization)	1
RPC STATD UDP stat mon_name format string exploit attempt	1
RPC portmap request status	1

Παρατηρούμε ότι σε μεγάλο ποσοστό τα alerts έχουν να κάνουν με pings. Το ping είναι ίσως το πρώτο βήμα πριν από κάθε απόπειρα για εισβολή, αφού με αυτό διαπιστώνει κανείς αν ένας host είναι up , οπότε και συνήθως συνεχίζει με κάποιο port scanning. Το ίδιο ισχύει και για τα autorooters [5] που είναι προγράμματα που αυτόματα ψάχνουν μεγάλα ranges δικτύων για συγκεκριμένες ευπάθειες τις οποίες καταγράφουν .

Πέρα από το απλό ping που εγκαθιστά κανονική και ολοκληρωμένη σύνδεση υπάρχουν πολλές ακόμα τεχνικές που κάνουν πιο αποδοτική την προσπάθεια για ανεύρεση ζωντανών hosts. Υπάρχει το Stealth SYN scan, το FIN scan, το Xmas Tree scan, το Null scan mode, το UDP scan, Window scan και άλλα τα οποία καταφέρνουν να περνούν απαρατήρητα από τα IDS συστήματα και επίσης να διαπιστώσουν αν ο host είναι ζωντανός σε περιπτώσεις που το απλό ping scan αποτυγχάνει [6] ,όπως για παράδειγμα τα SYN scans τα οποία συχνά φιλτράρονται αυτόματα από τα firewalls.

Ένα μεγάλο μέρος από τα alerts -περίπου το 1/6 -έχει σαν στόχο τα λειτουργικά της microsoft και συγκεκριμένα τις πόρτες 135, 139 και 445 που χρησιμοποιούνται από το

netbios, ή τις πόρτες 5554 και 8967 που σχετίζονται με δραστηριότητα worms. Μπορούμε να κάνουμε αναζήτηση με τη βοήθεια του acid με βάση την destination port και να μας επιστρέψει τα alerts που προορίζονται για τη συγκεκριμένη πόρτα. Έτσι μπορούμε να αναζητήσουμε στο internet πληροφορίες για το alert που μας ενδιαφέρει, να δούμε από που προέρχονται οι επιθέσεις, ποιοι από τους hosts μας δέχτηκαν τις επιθέσεις, ή να ψάξουμε για κάποιο *συγκεκριμένο περιστατικό.*



Εικόνα 5.6-unique alerts για την πόρτα 445

Παρατηρούμε επίσης ότι δεν υπάρχουν alerts για τον apache web server. Αν λάβουμε υπόψιν το μεγάλο ποσοστό χρήσης του apache στο internet, το οποίο είναι 69.6% σε αντίθεση με το 20.53% του iis [7],βεβαιωνόμαστε για μια ακόμη φορά για το γεγονός ότι ο apache είναι πολύ πιο ασφαλής από οποιονδήποτε άλλο web server χρησιμοποιείται στο διαδίκτυο!

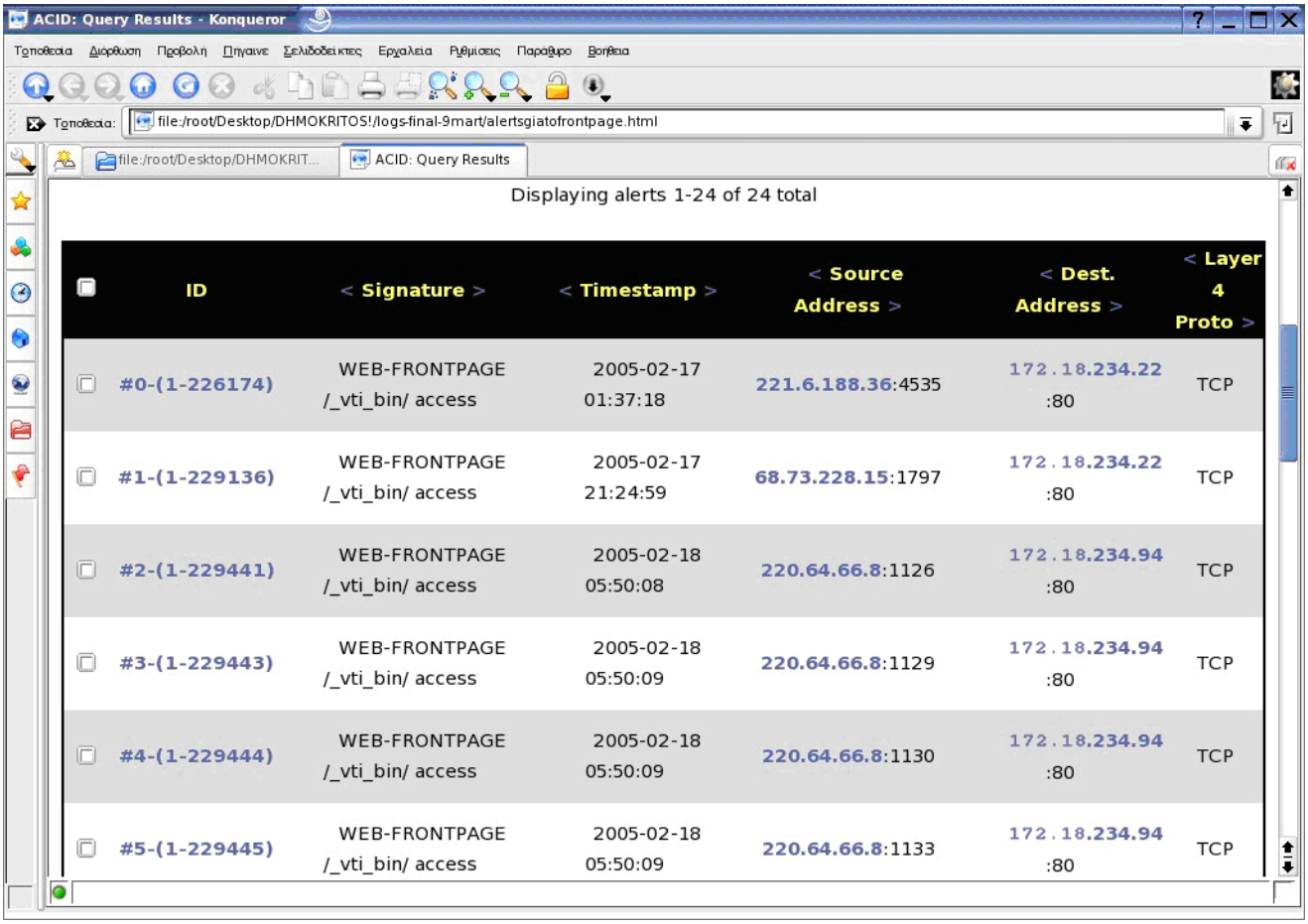
Αντίθετα υπάρχουν πολλά alerts για vulnerabilities που στοχεύουν τον web server της microsoft, τον iis. Αυτά είναι τα:
web iis view source via translate header [13]
WEB-FRONTPAGE rad fp30reg.dll access [11]

WEB-MISC webdav search access [14]
WEB-IIS cmd.exe access WEB-IIS ISAPI .ida attempt [12]
WEB-IIS multiple decode attempt
WEB-IIS CodeRed v2 root.exe access [15]
WEB-IIS unicode directory traversal attempt [16,17]
WEB-FRONTPAGE /_vti_bin/ access
WEB-IIS _mem_bin access
WEB-IIS Unicode2.pl script (File permission canonicalization)

Κάποια από τα παραπάνω είναι διάρκειας αρκετών χρόνων, όπως για παράδειγμα το unicode που είναι από το 2000 και όμως εξακολουθούν να υπάρχουν! Αυτό οφείλεται στο γεγονός ότι ακόμα και μετά από 3-4 χρόνια κυκλοφορίας ενός vulnerability στο internet, υπάρχουν ακόμα υπολογιστές που τρέχουν την υπηρεσία, όσο παλιά και αν είναι. Τα συγκεκριμένα vulnerabilities του iis οφείλονται για το τεράστιο ξέσπασμα παραβιάσεων σε windows servers που ξεκίνησε από το 2000 και φυσικά συνεχίζεται μέχρι σήμερα.

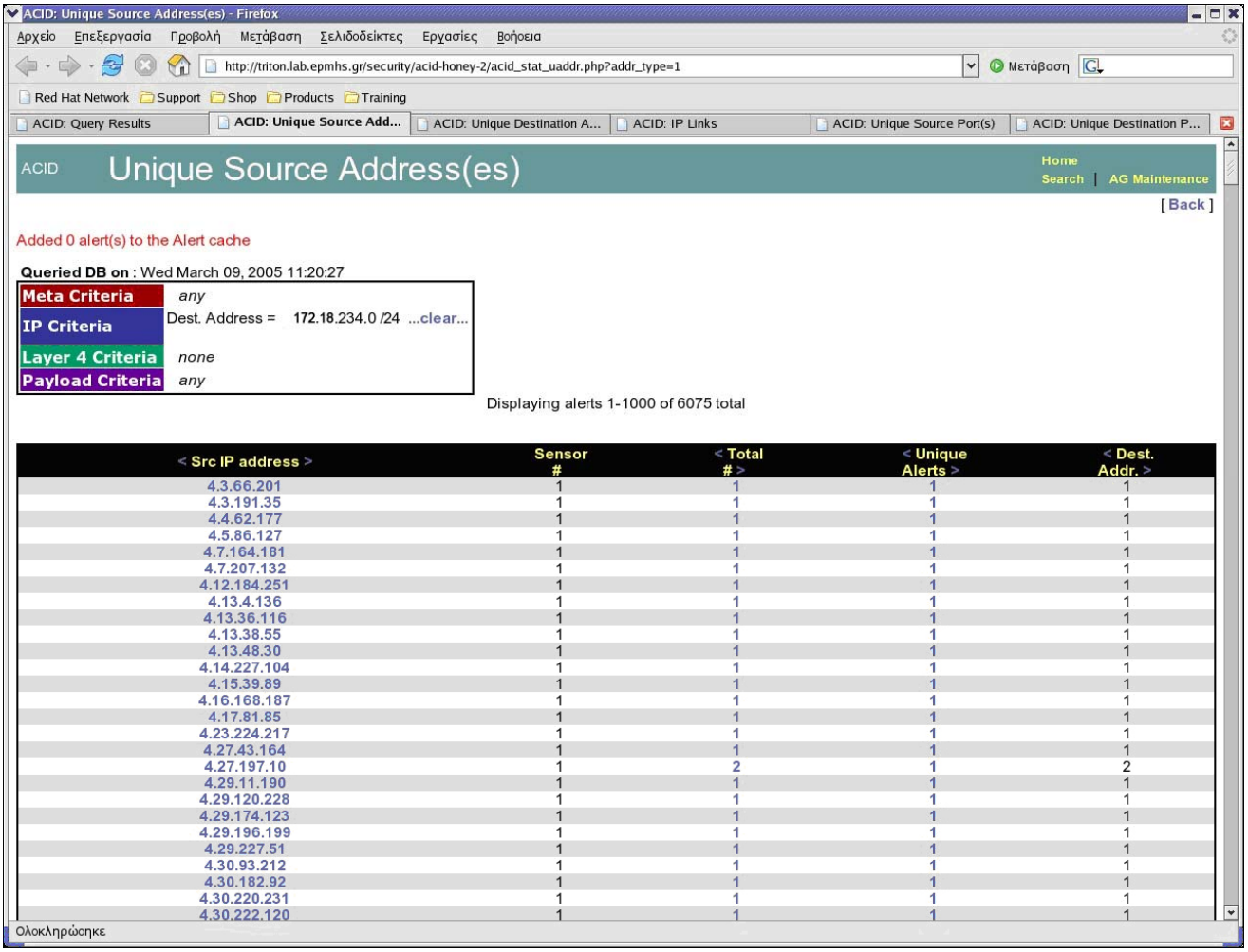
Είναι τόσο εύκολο να παραβιαστεί ένας windows server που τρέχει κάποια ευάλωτη έκδοση του iis που θα μπορούσε να το κάνει οποιοσδήποτε διαθέτει έναν browser!

Κρίνοντας από το πόσο ενεργές είναι ακόμα οι επιθέσεις για τον iis ακόμα και 5 χρόνια από τότε που κυκλοφόρησαν, βεβαιώνεται κανείς ότι δεν υπάρχει περίπτωση ένας unpatched iis web server να μην ανακαλυφθεί από script kiddies και autorooters και φυσικά να παραβιαστεί.



Εικόνα 5.7-alerts για το web-frontpage /vti_bin/access

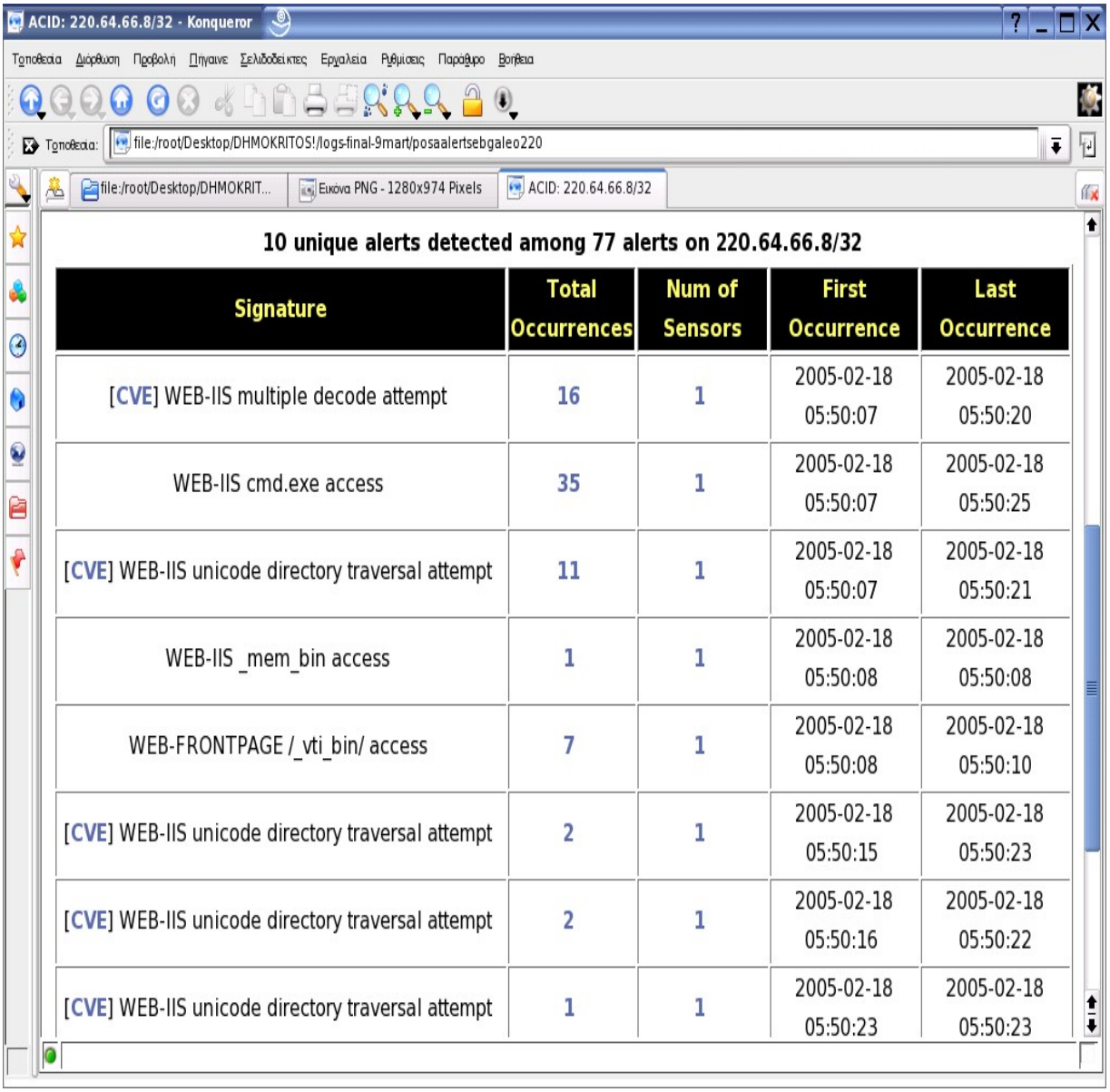
Μπορούμε να κάνουμε αναζήτηση με βάση τους εισερχόμενους hosts ώστε να βρούμε τα alerts για κάποια συγκεκριμένη ip, όπως φαίνεται στις παρακάτω εικόνες:



Εικόνα 5.8-unique source addresses

Πατώντας σε κάποια από τις ip's το acid θα μας βγάλει πληροφορίες για το ποια alerts προκάλεσε η συγκεκριμένη ip, τη συχνότητα αυτών, και τον χρόνο που συνέβηκε η καθεμία. Στην επόμενη εικόνα βλέπουμε για παράδειγμα οτι ο 220.64.66.8 έχει προσπαθήσει να παραβιάσει τους virtual hosts μας δοκιμάζοντας 77 exploits που εκμεταλλεύονται κάποιες από τις τρύπες του iis. Προφανώς και οι επιθέσεις δεν έχουν γίνει με χειρωνακτικό τρόπο, παρά αυτόματα με χρήση κάποιου προγράμματος autorooter.

Αν θέλουμε να βρούμε που εντοπίζεται αυτή η ip μπορούμε να κάνουμε αναζήτηση στο APIN[8], το οποίο είναι το american registry for internet numbers. Το ARIN μας ενημερώνει οτι η διεύθυνση αυτή είναι κατοχυρωμένη από το APNIC[9], το asia pacific network information center, από το οποίο και μαθαίνουμε ότι η ip 220.64.66.8 εντοπίζεται στην Νότια Κορέα, στη Σεουλ. Αν θέλουμε να μάθουμε περισσότερα για το δίκτυο στο οποίο βρίσκεται μπορούμε να επισκεφτούμε την υπηρεσία whois για την Κορέα[10]. Το γεγονός ότι η επίθεση έγινε από ip στην Κορέα δε μας ξενίζει καθόλου. Η Κορέα είναι μια από τις χώρες παραδείσους στα τρύπια συστήματα, από την πλευρά της ασφάλειας δικτύων και πιθανότατα πρόκειται για κάποιο παραβιασμένο μηχάνημα!



10 unique alerts detected among 77 alerts on 220.64.66.8/32

Signature	Total Occurrences	Num of Sensors	First Occurrence	Last Occurrence
[CVE] WEB-IIS multiple decode attempt	16	1	2005-02-18 05:50:07	2005-02-18 05:50:20
WEB-IIS cmd.exe access	35	1	2005-02-18 05:50:07	2005-02-18 05:50:25
[CVE] WEB-IIS unicode directory traversal attempt	11	1	2005-02-18 05:50:07	2005-02-18 05:50:21
WEB-IIS _mem_bin access	1	1	2005-02-18 05:50:08	2005-02-18 05:50:08
WEB-FRONTPAGE /_vti_bin/ access	7	1	2005-02-18 05:50:08	2005-02-18 05:50:10
[CVE] WEB-IIS unicode directory traversal attempt	2	1	2005-02-18 05:50:15	2005-02-18 05:50:23
[CVE] WEB-IIS unicode directory traversal attempt	2	1	2005-02-18 05:50:16	2005-02-18 05:50:22
[CVE] WEB-IIS unicode directory traversal attempt	1	1	2005-02-18 05:50:23	2005-02-18 05:50:23

ΣΗΜΕΙΩΣΕΙΣ -ΠΑΡΑΠΟΜΠΕΣ

[1] http://www.snort.org

[2] http://netfilter.org

[3] http://www.ethereal.com

[4] http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html

[5] Introduction to autorooters:crackers working smarter, not harder
http://www.securityfocus.com/infocus/1619

[6] The art of port scanning, by fyodor
http://www.insecure.org/nmap/nmap_doc.html

[7] Netcraft web server syrvey, http://news.netcraft.com

[8] American registry for internet numbers, http://ws.arin.net

[9] Asia pacific network information center, http://www.apnic.net

[10] Korean whois service,
http://whois.nida.kr/whois

[11] http://www.securityfocus.com/bid/9007
[12] http://www.securityfocus.com/bid/1065
[13] http://www.securityfocus.com/bid/1578
[14] http://www.whitehats.com/info/ids474
[15] http://www.cert.org/advisories/CA-2001-19.html
[16] http://www.securityfocus.com/bid/1806

[17] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0884

[18] bleeding snort rules
http://www.bleedingsnort.com

[19] http://www.snort.org/docs/setup_guides/snort_base_SSL.pdf

Snort, Apache, SSL, PHP, MySQL, and BASE Install on CentOS 4 (or RHEL 4)

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

[21]“ISLAB HACK: Βασικές Έννοιες & Προγραμματισμός του SNORT 2.0” του Δημήτρη Πρίτσου, πτυχιακή εργασία, διαθέσιμη online http://www.islab.demokritos.gr