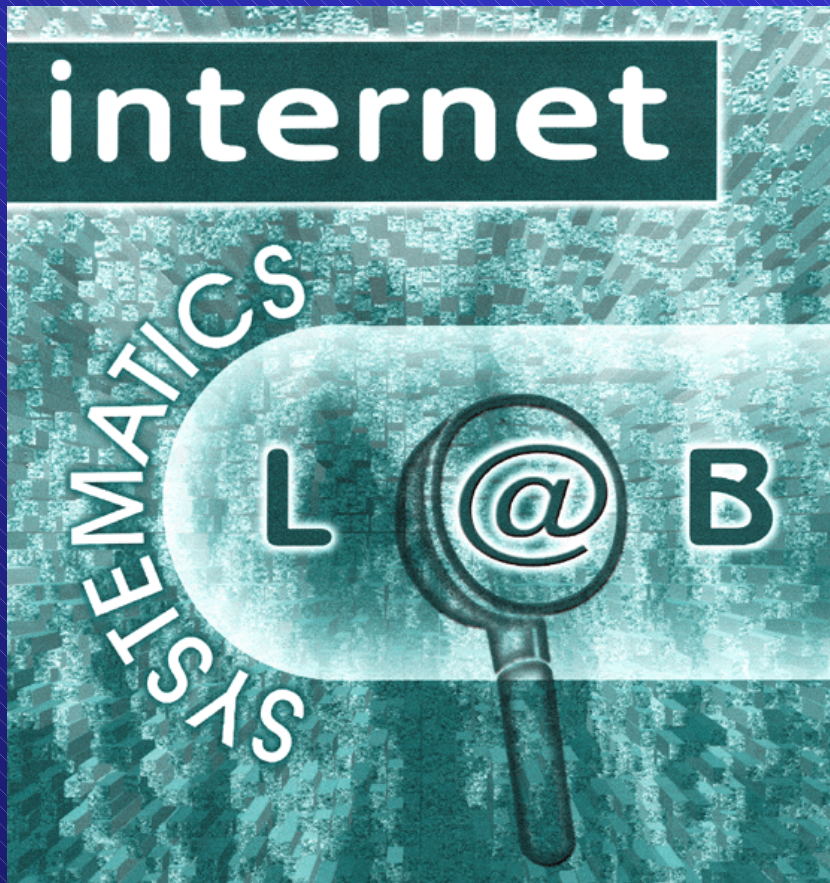


Διαχείριση Γνώσης

ΟΜΙΛΗΤΗΣ: Δρ. Ιωάννης Κοροβέσης
Εργαστήριο: Internet Systematics Lab

ΚΗΥ/ΜΟΝΑΔΑ ΔΙΚΤΥΩΝ



ΕΘΝΙΚΟ
ΚΕΝΤΡΟ
ΕΡΕΥΝΑΣ
ΦΥΣΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ
“ΔΗΜΟΚΡΙΤΟΣ”



Διαχείριση Γνώσης με CMS

The screenshot displays the Internet Systematics Lab (INTRA) CMS interface. At the top, there is a navigation bar with the site name, a search box, and a topics dropdown menu. Below this is a secondary navigation bar with a welcome message and a date. The main content area features a 'Web Admin Message' section with a text-based announcement. Below the message are three article snippets, each with a thumbnail image, a title, a post date, and a 'Read more...' link. The right sidebar contains several widget boxes: a Google Search box, a Categories Menu, a Today's Big Story box, and a Past Articles list. The left sidebar contains a Main Menu and an Operations Support section.

Internet Systematics Lab (INTRA)

Search topics **ALLTOPICS**

Welcome Admin! | [logout](#) | May 12, 2005

Main Menu

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

Contents

- News
- Topics Map
- Reviews - HowTo - WhatIs
- 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

Web Admin Message

Για την καλύτερη χρήση του εσωτερικού μηχανισμού μηνυμάτων προτινεται 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 καθαρά δικό μου κώδικα που αφορά αναζήτηση συγκεκριμένου substring μέσα στο string. Με αυτό τον τρόπο θα μπορώ να κάνω ένα multilayer 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 τον κώδικα που μου χρειάζεται για την πτυχιακή μου από το mod_detect.c του apache sever. Πληροφοριακά για όσους δεν παρακολουθούν την πτυχιακή 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 shows a web forum interface with a central content area and sidebars on the left and right. The central area contains three posts:

- Private Msg**: Posted by Admin on (0 Reads). The post text discusses a messaging issue in 'intra_pn' and includes a code snippet:

```
//Added by dpritsos : 1700 = 30min  
echo("<meta http-equiv='refresh' content='1700;url=http://triton.lab.epmhs.gr/intra_pn^>");
```
- Data Analysis Articles**: Posted by elgar on (3 Reads). The post features a penguin icon and the text '0-1100'. It discusses 'Anti-IDS Tools and Tactics' and provides a link to <http://www.sans.org/rr/intrusion/anti-ids.php>.
- Updated HnDatabaseFix**: Posted by elgar on (4 Reads). The post features a 'The Honeynet' logo and discusses a bug fix for 'spp_portscan'.

The left sidebar contains navigation menus for 'Looking Glass', 'Research Systems', 'Links', and 'Incoming'. The right sidebar contains 'Who's Online' (showing 1 guest and 2 members) and 'Languages' (set to 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)

Welcome Admin! | logout | May 12, 2009

Search topics **ALLTOPICS**

Main Menu

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

Contents

- News
- Topics Map
- Reviews - HowTo - WhatIs
- 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	 The Honeynet BookChapter5-genII	 Προσमितες/Συνεργασίες
 Hn Bridge2	 Snort Module Project (από Παναγιώτο)	 Ψάξιμο και ανάπτυξη διαφόρων tools	 Open NMS	 Operational Ariadne-t
 Building our Sites	 Προτάσεις για tasks,πτυχιακές 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^α

Open NMS



Operational Ariadne-t



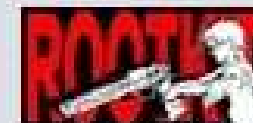
Bulding our Sites



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	Εργασία που ελήφθη...		09/21/2001		09/21/2001	
CH:0, FO: 2			13:46		18:33	
▶ 319	Εργασία που ελήφθη...		09/21/2001		09/25/2001	
CH:0, FO: 4			19:06		13:25	
▶ 320	Εργασία που ελήφθη...		09/25/2001		09/25/2001	
CH:0, FO: 2			13:29		13:30	
▶ 321	Εργασία που ελήφθη...		09/25/2001		09/25/2001	
CH:0, FO: 4			13:37		13:42	
▶ 322	Εργασία που ελήφθη...		09/26/2001		10/31/2001	
CH:0, FO: 1			16:24		13:03	
▶ 323	Εργασία που ελήφθη...		09/27/2001		02/04/2002	
CH:0, FO: 6			13:29		15:48	
▶ 324	Εργασία που ελήφθη...		09/27/2001		12/12/2001	
CH:0, FO: 2			13:31		15:28	
▶ 326	Εργασία που ελήφθη...		09/28/2001		10/05/2001	
CH:0, FO: 10			11:22		17:09	
▶ 327	Εργασία που ελήφθη...		09/28/2001		09/16/2002	
CH:0, FO: 23			12:22		22:13	
▶ 328	Εργασία που ελήφθη...		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 <https://> Go Search Print

Home Bookmarks Mozilla Stuff [i-mag](#) [Key](#) Enter search term, keyword, or web address [Ariadne-t 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 143.233.36.38 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



Monitored Hosts

All monitored hosts 

Monitored Files

All monitored files 

Alerts (Last 6 Hrs)

Time	Count
11 AM (16914)	
10 AM (21767)	
9 AM (19457)	
8 AM (15577)	