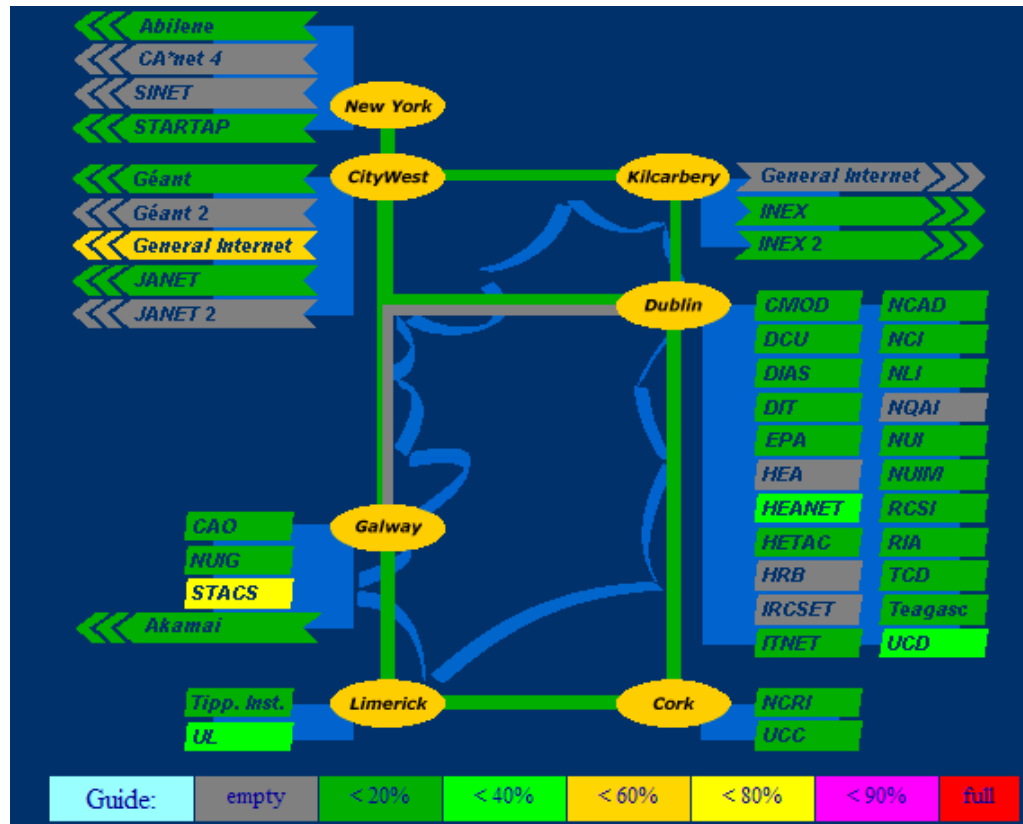




# **Building Security into our Infrastructure: HEAnet Security Services**

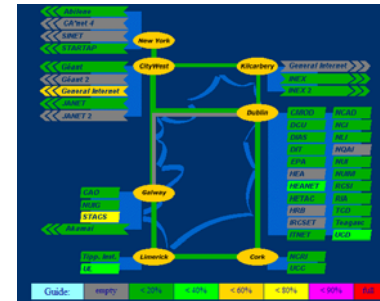
Warren Daly – HEAnet

# Expanding Infrastructure



# Netflow

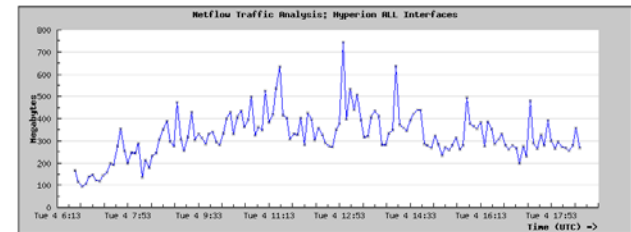
- Detailed traffic statistics
- Malicious code detection



NETFLOW VERSION 0.8

USERID: 1  
USERNAME: heanet

A.S. STATS IN  
A.S. STATS OUT  
NODE\_STATS

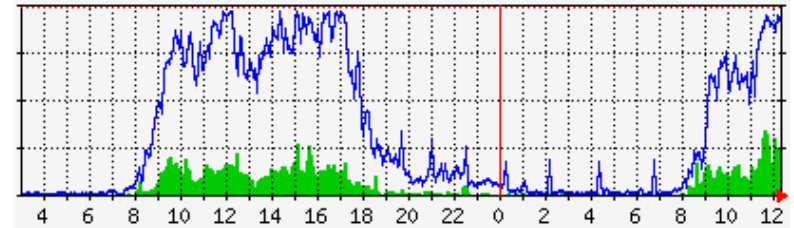


Source Address	T	W	Source Port	SAS	Destination Address	T	W	Dest Port	OAS	Timestamp	Bytes
Alkamais.haa.net	T	W	80	0	firewall.netloo.ie	T	W	26997	0	Tue 10:20	167892632
Alkamais.haa.net	T	W	80	0	firewall.netloo.ie	T	W	26997	0	Tue 10:22	22006479
ehras6.ucc.ie	T	W	4336	0	131.211.218.104	T	W	8881	20365	Tue 10:28	16441544
ehras6.ucc.ie	T	W	4336	0	131.211.218.104	T	W	8881	20365	Tue 10:33	14993725
Alkamais.haa.net	T	W	80	0	net.loo.ie	T	W	3746	0	Tue 10:33	14348650
www.rca.ie	T	W	443	0	sec02.usam.usg.bh	T	W	1261	11537	Tue 10:28	13087854

# D/DoS Detection (zazu)

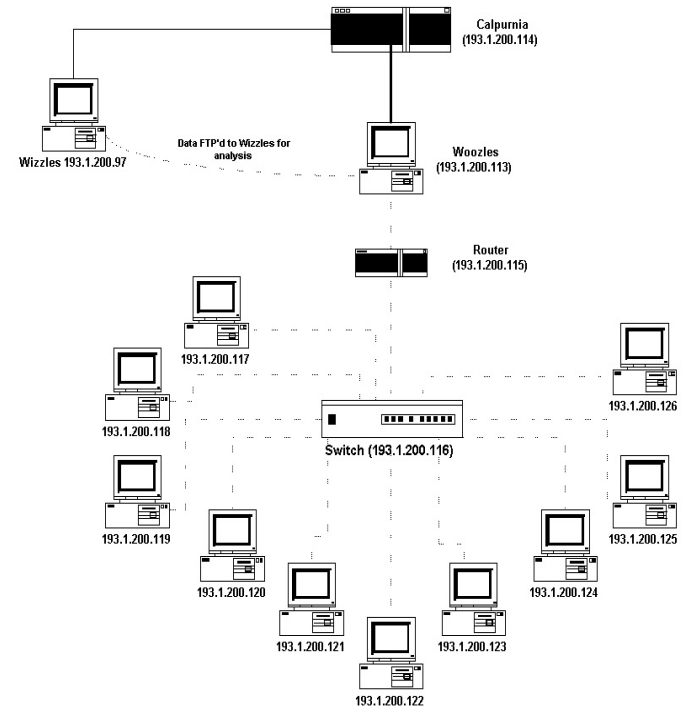


- Modular
- Operation
- ICMP attacks
- UDP DoS attacks
- Syn Flood DoS



# Honeypot

- Flexible & Advanced
- Reduce false positives
- Tracking internal problems



# Advice & Reporting

- Warnings
- Advice
- Tracking

Mousetrap 3.0

**Ticket #20031105-3**

Status:  Scheduled:

Owner:  Distribution:

Resolver:  Site/Line/Pop:

Problem Start:   Problem End:

Subject:

To:

Cc:

Bcc:

Problem:

**Ticket #20030923-7 (wdaly)**

To: heanet-tech-security@listserv.heanet.ie  
From: Warren Daly <warren.daly@heanet.ie>  
Subject: HEA-NOC/20030923-7 SECURITY Apple Security update for vulnerabilities  
X-HEANet-TicketID: 20030923-7  
X-HEANet-Ticket-Distribution: security  
Message-ID: <20030923-7-18mousetrap.heanet>

Ticket Number: HEA-NOC/20030923-7      Ticket Status: SECURITY  
Ticket Type: unscheduled      Resolver:  
Ticket Opened: 20030923 14:25 UTC+1      Problem Start: 20030923 14:20 UTC+1  
Ticket Closed: 20030923 14:25 UTC+1      Problem End:

Site/line: Security

Problem Description:  
Vulnerabilities in OpenSSH, Sendmail, fd\_realpath  
and explookup.


Information will also be posted to the Apple Product Security web site:  
[http://www.apple.com/support/security/security\\_updates.html](http://www.apple.com/support/security/security_updates.html)

# Conclusion

- Multiple Systems
- Prevention
- Proactive

# Suggestions

- [noc@heanet.ie](mailto:noc@heanet.ie)
- (01) 6609040



---

# Information Security: Policies & Cybercrime

Warren Daly – HEAnet

# Security Policies

- Framework
- Legislation

# Framework

- Guidelines
- React
- Support

# Information Security Policy

- Its purpose and scope
- Guidelines and procedures for everyday security practice
- A definition of responsibilities
- Clear emergency procedures
- Appropriate, enforceable sanctions
- References to supplementary documents

# Legislation

- Data Protection
- Computer Misuse & Legal Framework

# Incident Descriptions

- **Computer Fingerprinting**
- **Malicious Code**
- **Denial of Service**
- **Account Compromise**
- **Intrusion Attempt**
- **Unauthorised Access to Information**
- **Unauthorised Access to Transmissions**
- **Unauthorised Modification of Information**
- **Unauthorised Access to Communication Systems**

# Legislative Procedures

Incident	Ireland
Target Fingerprinting	n.a
Malicious Code	n.a
Denial of Service	n.a
Account Compromise	Criminal
Intrusion Attempt	Criminal
Unauthorised access to Information	Criminal
Unauthorised access to transmissions	n.a
Unauthorised modification of Information	n.a
Unauthorised access to communications system	Criminal

# Legislation

- (CoE) Convention on Cybercrime
- Data Protection Act (1998 & 2003)
- Criminal Damages Act 1992 (Sec 5)

- Questions?