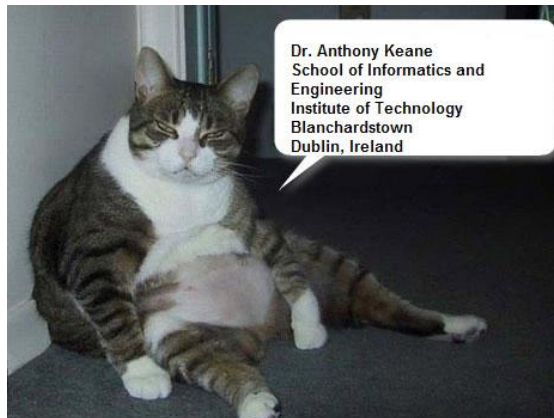


HONEYNETS AND DARKNETS

WHAT GOOD ARE THEY?

11:20-11:50am Friday, November 14th, 2008

Presented by



and



Aidan Carty
HEAnet

Content

- Introduction and Overview
- Honeynet activities at ITB
- Honeynet activities at HEAnet

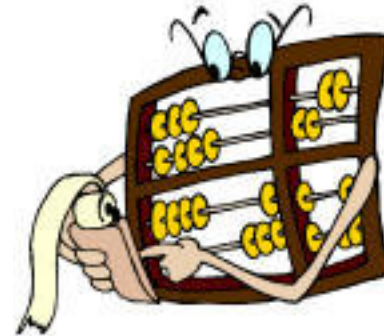
The Problem

Computer Crime – To make lots of money £\$€

- Botnets
- DDoS
- theft of data and information
- identity theft

Business attacks cost money

- down time of services
- negative publicity
- poor business confidence in service and products
- compliance



What are the Security Risks?

SANS Top-20 2007 Security Risks (2007 Annual Update)

Client-side Vulnerabilities in:

- C1. Web Browsers
- C2. Office Software
- C3. Email Clients
- C4. Media Players

Server-side Vulnerabilities in:

- S1. Web Applications
- S2. Windows Services
- S3. Unix and Mac OS Services
- S4. Backup Software
- S5. Anti-virus Software
- S6. Management Servers
- S7. Database Software

Security Policy and Personnel:

- H1. Excessive User Rights and Unauthorized Devices
- H2. Phishing/Spear Phishing
- H3. Unencrypted Laptops and Removable Media

Application Abuse:

- A1. Instant Messaging
- A2. Peer-to-Peer Programs

Network Devices:

- N1. VoIP Servers and Phones

Zero Day Attacks:

- Z1. Zero Day Attacks

Best Practices for Preventing Top 20 Risks

<http://www.sans.org/top20/>

Ten key findings

Ernst & Young Global Information Security Survey 2008

1. Protecting reputation and brand has become a significant driver for information security.
2. Despite economic pressures, organizations continue to invest in information security.
3. International information security standards are gaining greater acceptance and adoption.
4. Many organizations still struggle to achieve a strategic view of information security.
5. Privacy is now a priority, but actions are falling short.
6. People remain the weakest link for information security.
7. Growing third-party risks are not being addressed.
8. Business continuity is still bound to information technology.
9. Most organizations are unwilling to outsource key information security activities.
10. Few companies hedge information security risks with cyber insurance.



"The virus was contained in an e-mail warning about the virus ..."

Monitoring Computer Attacks and Network Activity

*“While I nodded, nearly napping, suddenly there came a tapping,
as of someone gently rapping, rapping at my chamber door.”*

Edgar Allen Poe

Places to look at for malicious or illegal behaviour:

- Gateway boundary to network
- Inside network
 - Server
 - Client Computer
 - Database with false records
- Wirelessly access

So how can we detect and monitor attacks?

Honeynets and Darknets



Definitions

A **Honeynet** is a high-interaction honeypot designed to capture extensive information on threats. Honeynets are real systems, applications, and services made available to see how they are attacked. www.honeynet.org

A **Darknet** is a portion of routed, allocated IP space in which no active services or servers reside. These are "dark" because there is, *seemingly*, nothing within these networks. www.team-cymru.org/

Motivation

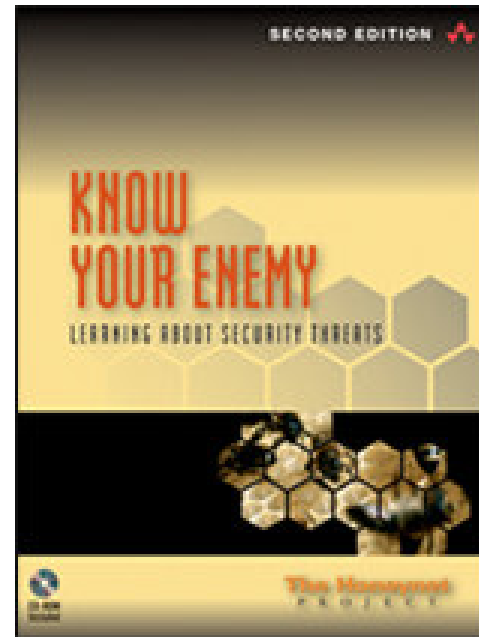
To understand the attacks

- what tools are used
- how are they used
- by whom
- and why

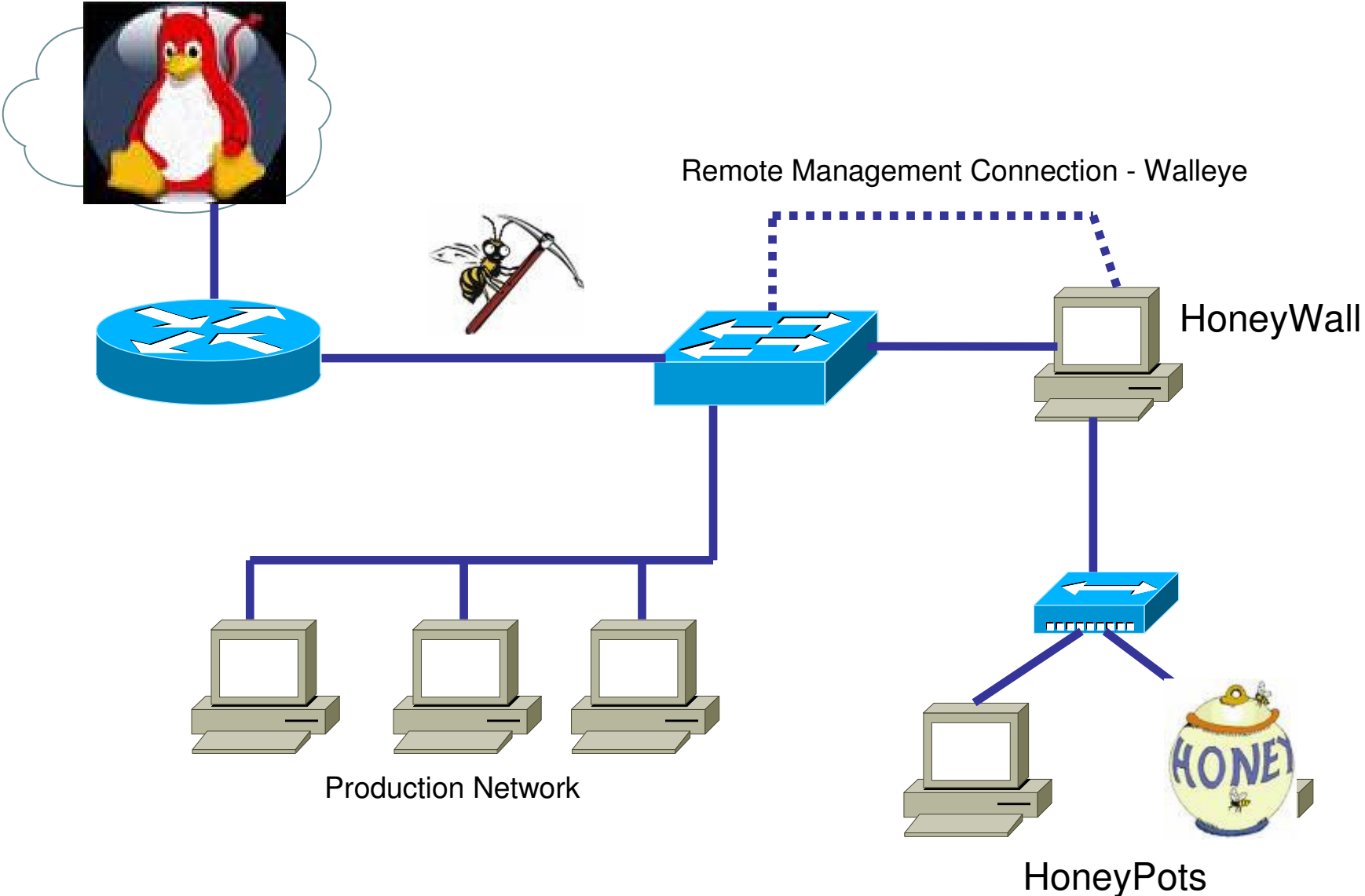
Tactics and Motives

Honeynet Types

- High Interaction
- Low Interaction
- Virtual Honeynets
- Distributed Honeynets



HoneyNet Architecture in IT Blanchardstown



Honeynet Configuration

Main configuration items:

1. Mode and IP Information

- Honeynet mode (bridged only)
- Honeynet IP address
- External and Internal Bridge Interface
- LAN broadcast
- LAN CIDR

2. Remote Management

- IP address and subnet of honeypots
- Gateway address
- Hostname, Domain name and DNS
- Manager IP address
- Restriction on inbound / outbound traffic
- Walleye (activate option)

Honeynet Operation

Data Control

- Containment of activity
- Monitor inbound/outbound connections
- Automatic alerting
- Ability to block outward bound activity – *very important!*
- *Difficult for attackers to detect* (???)

Data Capture

- monitoring / logging of all activities / data
- challenge is to collect as much data as possible without being detected
- layers
 - Firewall – logs – alert ~IDS - IPTables
 - IDS – full binary data capture of network traffic – Snort-Inline
 - Honeypot – syslogd – Sebek – capture keystrokes



All traffic on a Honeynet is considered

malicious and goes through:

- **data control firewall**

- **tracks connections**

- **intrusion protection system (IPS)**

- **drops or modifies malicious traffic**

Main Advances

- All traffic is suspicious
- Collect small data sets
- Reduce false positives
- Catch false negatives
- Capture encrypted activity
- Works with IPv6
- Highly flexible
- Requires minimum resources

Data Analysis
System Admin
Logout

Online Honeywalls

Honeywall: 168430146 Created: Tue May 8 14:52:07 2007 Last Update: Fri Jun 29 12:24:04 2007

	Bidirectional Flows				Total Flows			
	In		Out		In		Out	
	con	ids	con	ids	con	ids	con	ids
1 Hour	0	0	0	0	0	0	0	0
24 Hour	0	0	0	0	0	0	0	0

Honeywall: ITB-AJK1 Created: Mon Jul 2 10:37:37 2007 Last Update: Sun Dec 2 15:16:30 2007

	Bidirectional Flows				Total Flows			
	In		Out		In		Out	
	con	ids	con	ids	con	ids	con	ids
1 Hour	0	0	0	0	36	0	16	0
24 Hour	0	0	0	0	1,333	4	322	0

Search (short term soln)

Time Start: End:

IP Proto:

Either Prefix: Port:

Source Prefix: Port:

Destination Prefix: Port:

Result Format:

Honeywall Details for 3238119782

Sensor ID:	3238119782	Sensor Name:	Honeywall: ITB-AJK1
Install Date:	Mon Jul 2 10:37:37 2007	Last Update:	Tue Dec 4 18:31:29 2007
State:	online		
Country:	IE	Timezone:	0
Latitude:		Longitude:	
Network Type:	com		
Notes:			

Activity Report

Top 10 Honeypots				Top 10 Remote Hosts			
Flags	Host	Connections	IDS events	Host	Connections	IDS events	
	193.1.201.99	334	0	58.20.228.52	4	3	
	193.1.201.102	14	0	62.202.42.149	29	0	
				193.194.85.74	7	0	
				24.64.98.137	6	0	
				221.208.208.99	6	0	
				221.208.208.93	5	0	
				221.208.208.96	5	0	
				218.10.137.142	5	0	
				218.10.137.141	5	0	
				75.191.204.231	4	0	
Top 10 Source Ports				Top 10 Destination Ports			
Port	Connections	IDS events		Port	Connections	IDS events	
1376	4	3		1434	9	3	
138	202	0		1026	421	0	
137	119	0		1027	378	0	
0	41	0		1028	351	0	
31074	20	0		138	202	0	
31077	18	0		137	119	0	
48186	8	0		135	56	0	
6000	7	0		0	41	0	
32814	7	0		445	36	0	
20251	6	0		80	15	0	

(Previous Page)	Start	7	8	9	10	11	12	13	14	15	16	17	18	19	20
December 1st 15:06:40	89.171.150.48	00:00:00	->	193.1.201.100											
ICMP ECO	0 os unkn	0 kB 1 pkts -->	<--0 kB 0 pkts	0											
December 1st 15:09:23	82.178.22.22	00:00:00	->	193.1.201.102	<-1-MS-SQL Worm propagation attempt										
UDP INT	63208 os unkn	0 kB 1 pkts -->	<--0 kB 0 pkts	ms-sql-m	<-1-MS-SQL version overflow attempt										
December 1st 15:09:50	193.1.201.99	00:00:00	->	193.1.201.103											
UDP INT	netbios-dgm os unkn	0 kB 1 pkts -->	<--0 kB 0 pkts	netbios-dgm											
December 1st 15:13:04	63.192.170.101	00:00:03	->	193.1.201.99											
UDP INT	netbios-ns os unkn	0 kB 3 pkts -->	<--0 kB 0 pkts	netbios-ns											
December 1st 15:14:03		00:00:00	->												

UDP INT	netbios-dgm os unkn	0 kB 1 pkts -->	<--0 kB 0 pkts	netbios-dgm											
December 1st 16:25:53	61.157.96.108	00:00:00	->	193.1.201.100	<-1-MS-SQL Worm propagation attempt OUTBOUND										
UDP INT	2166 os unkn	0 kB 1 pkts -->	<--0 kB 0 pkts	ms-sql-m	<-1-MS-SQL Worm propagation attempt										
December 1st 16:26:03	193.1.201.99	00:00:00	->	193.1.201.103											

December 1st 16:25:53	61.157.96.108	00:00:00	->	193.1.201.100	<-1-MS-SQL Worm propagation attempt OUTBOUND										
UDP INT	2166 os unkn	0 kB 1 pkts -->	<--0 kB 0 pkts	ms-sql-m	<-1-MS-SQL Worm propagation attempt										
					<-1-MS-SQL version overflow attempt										
IDS details															
(Previous Page)	Start	1												End	(Next Page)
Timestamp	Priority	Classification	Type	Name	Revision	Generator	Reference								
December 1st 16:04:53	2	Misc Attack		MS-SQL Worm propagation attempt OUTBOUND	7	rules_subsystem	cve,2002-0649 bugtraq,5311 bugtraq,5310 nessus,11214 url,vil.nai.com/vil/content/v_99992.htm								
December 1st 16:04:53	2	Misc Attack		MS-SQL Worm propagation attempt	8	rules_subsystem	cve,2002-0649 bugtraq,5311 bugtraq,5310 nessus,11214 url,vil.nai.com/vil/content/v_99992.htm								
December 1st 16:04:53	3	Misc activity		MS-SQL version overflow attempt	7	rules_subsystem	bugtraq,5310 cve,2002-0649 nessus,10674								
Flow Examination															
Snort	Packet Decode														
Snort	Rule Evaluation														

Data Analysis
System Admin
Logout

Administration Menu

- ⊕ OS Administration
- ⊕ Honeywall Administration
- ⊖ Honeywall Configuration
 - IP Information
 - Remote Management
 - Connection Limiting
 - DNS Handling
 - Alerting
 - Snort-Inline
 - Honeywall Upload
 - Honeywall Summary
 - Black and White List
 - Sebek
 - Roach Motel Mode
 - Fence List
 - Data Management
 - Honeynet Demographics
- ⊖ System Status
 - Network Interface
 - Honeywall Config
 - Firewall Rules
 - Running Processes
 - Listening Ports
 - Snort_inline Alerts-fast
 - Snort_inline Alerts-full
 - Snort Alerts
 - System Logs
 - Inbound Connections
 - Outbound Connections
 - Dropped Connections
 - tcpdstat Traffic Statistics
 - Argus Flow Summaries
 - Tracked Connections
 - Documentation
- ⊕ Snort Rules Managemet
- Manage Users

Honeywall System Administration

Welcome to the System Administration section of your Honeywall Gateway. The following pages will allow you to view the status and configure your Honeywall gateway. For detailed information about the operation of the Honeywall, please refer to the [Online User's Manual](#).

Uptime	Users		Load Average		
			1 Min	5 Min	15 Min
1 day 2:24	0 users		0.29	0.20	0.07
total	used	free	shared	buffers	cached
Mem:	313	289	23	0	68
Swap:	509	0	509		

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/hda1	342M	103M	222M	32%	/
none	157M	0	157M	0%	/dev/shm
/dev/hda5	342M	11M	315M	4%	/home
/dev/hda8	46M	4.9M	39M	12%	/hw
/dev/hda7	244M	6.1M	225M	3%	/tmp
/dev/hda2	981M	417M	514M	45%	/usr
/dev/hda6	342M	11M	314M	4%	/usr/local
/dev/hda9	6.7G	118M	6.2G	2%	/var

DB Table	Count
argus	21959
command	0
ids	93
ids_sig	6694
os	28
process	0
process_to_com	0
process_tree	0
sbk_loss	0
sensor	2
sys_open	0
sys_read	0
sys_socket	0

All warfare is based on deception
Sun Tzu

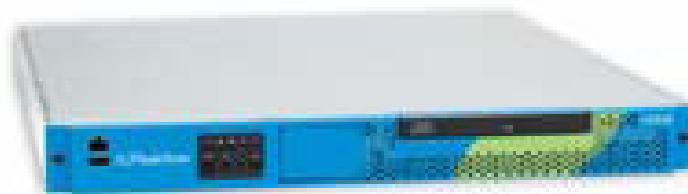
HEAnet use honeypots, Why ?



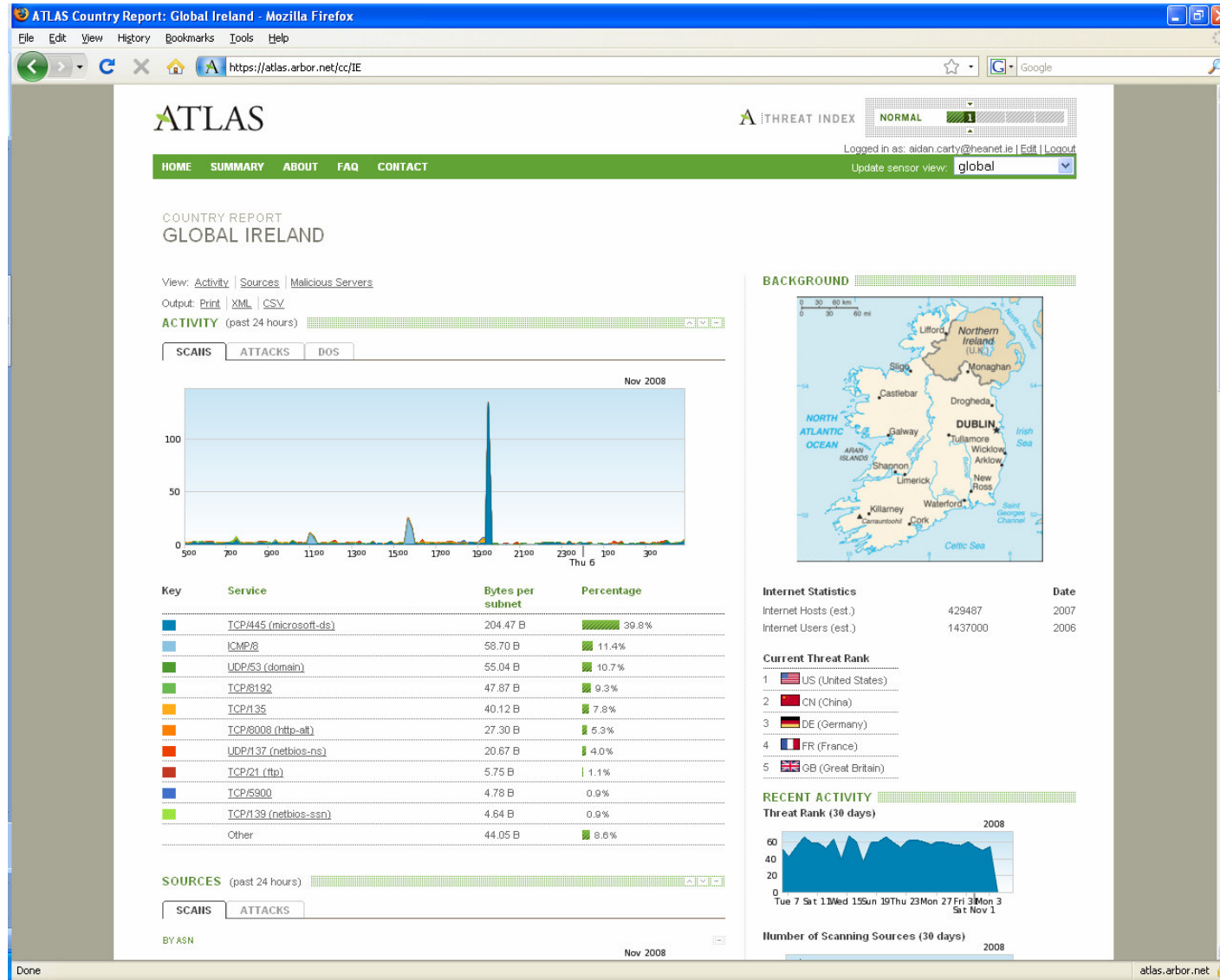
- Network Intelligence
- HEAnet Client Services
- Supporting the Security Community

Network Intelligence

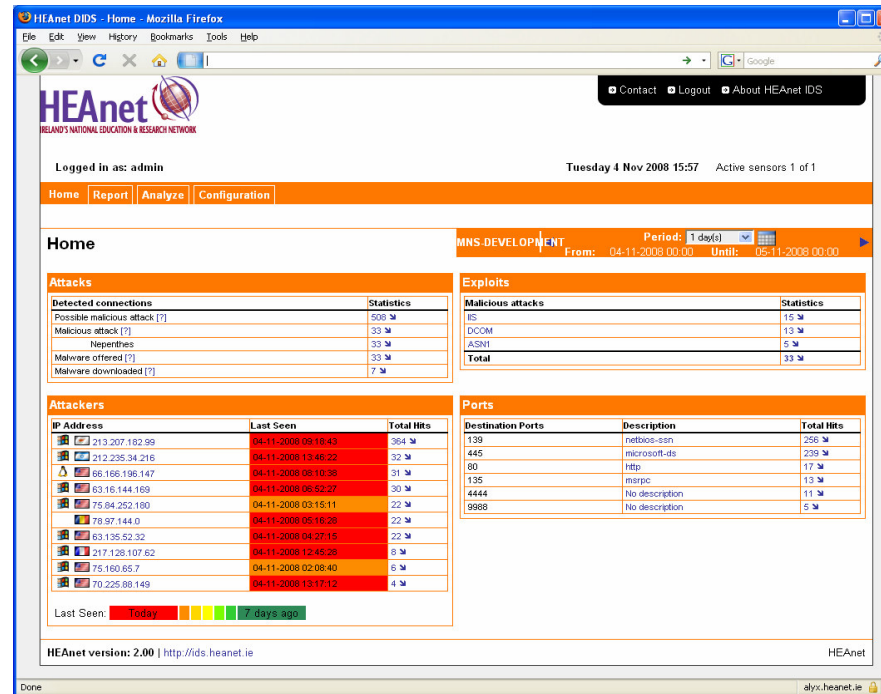
- Commercial vendor, ATLAS scheme
- Provides a view of HEAnet and Clients from other Tier-1 ISPs in US, ASIA and Europe
- Arbor work with non-for-profit organisations, “fighting the good fight”
- Provides reports and alerts of infected clients, including HEAnet clients
- Used by HEAnet NOC – is this port suspicious



What does it show



HEAnet Client Services



- HEAnet D-IDS services
- Honeypot for the community
- Provides early warning of infected machines e.g. Halls of residence or wireless lans

Security Community



- The Shadowserver Foundation
 - non-for-profit organisation
- Wombat Project
 - European FP7 project



Usefulness of Honeynets and Darknets

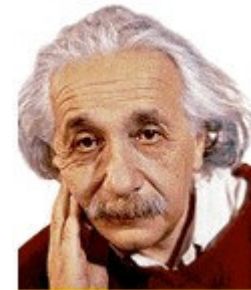
Education

- awareness
- gather real data for analysis



Research

- monitoring and analysing attacks over time
- detection of new attacks
- build better defences



Industry

- cheap IDS and IPS implementation
- prevention rather than cure



Any  Questions

