Honeypots and the Enterprise: Intelligence-based Risk Management

Institute for Security Technology Studies
Dartmouth College
Hanover, New Hampshire

George Bakos - gbakos@ists.dartmouth.edu
Hello. My name is....

- ISTS Distributed Honeypot Project
- DIB:S early worm detection
- IDABench intrusion analysis system
- Tiny Honeypot
- EWA-IIT
- Army National Guard Information Operations
- State of Vermont
What is a honeypot?

“a security resource whose value lies in being probed, attacked or compromised.”

-- Lance Spitzner

_Honeypots: Tracking Hackers_

“an information system resource whose value lies in unauthorized or illicit use of that resource.”
What do you care about?

Risk Management is:

“Decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.”

-- U Texas Medical Branch
Risk Management Strategies

1 - Accept exposure
   a. costs to remediate may outweigh ALE
   b. shrinkage

2 - Reduce exposure
   a. identify threats, identify vulnerabilities, remove vectors
   b. polish up your crystal ball!

3 - Transfer exposure
   a. is appropriate coverage available?
      i. possible?
      ii. palatable?
      iii. tenable?

Hint: That's what we're here for, folks!
What problems do honeypots solve?

Most security technologies are created with a specific purpose, in response to a particular problem.

Examples:
• Firewalls -- access control
• IDS's -- detection
What can honeypots do?

Honeypots are a more general technology, which can combat many different types of problems.

• Detect attacks
• Capture worms or malware in the wild
• Deter attacks
• Provide insight into attacker methods, motivations and technologies
So what gap do they fill?

Network IDS has a few chronic problems that honeypots address very well:

- False Positives
- False Negatives
- Volume
False Positives

An untuned IDS will alert way too much on normal network traffic in most organizations.

Soon, those alerts get ignored or the rules triggering them are pruned or modified.

But now we miss real attacks....
False Negatives

Your IDS usually doesn't fire on an attack if:

• The attack is completely new or at least too recent for your vendor.
• The rule matching it caused too many false positives.
• It's seeing too much traffic and dropping packets.
A serious problem in the IDS space lately is VOLUME.

Networks are getting faster, producing a much greater volume of data to analyze. Further, most IDS's can't cope with a heavily loaded gigabit network -- they start dropping packets.

There's just too many alerts to handle -- some get dropped by the humans.
Honeypots address all three

A honeypot has no production purpose, so:

Every bit of traffic sent to a honeypot is almost certainly hostile, meaning that there are almost no false positives.

(We say that while honeypots collect little data, the data they collect is highly valuable.)
Honeypots address all three

A honeypot can alert on every single incoming packet, reducing false negatives dramatically.

A stand-alone honeypot gets a very small volume of high-fidelity data, usually under 1 megabyte per day.
Isn't Network IDS enough?

[**] [1:618:2] SCAN Squid Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-08:09:27.772993 216.218.184.2:3704 -> 10.2.87.142:3128
TCP TTL:49 TOS:0x0 ID:35607 IpLen:20 DgmLen:44 DF
******S* Seq: 0x13C82726 Ack: 0x0 Win: 0x4000 TcpLen: 24
TCP Options (1) => MSS: 1412

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from
216.218.184.2 (THRESHOLD 4 connections exceeded in 0 seconds)
[**]
11/04-20:19:09.882416
Snort Network Intrusion Detection System alert
http://www.snort.org
Isn't Network IDS enough?

GET http://216.218.184.9/pI9Ob6SZcWQR2ODUWOopFg/\textcolor{red}{3128}/10-2-87-142 HTTP/1.0
Connection: close
Pragma: no-cache
Accept: text/html
Host: 216.218.184.9
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; AOL 5.0; Windows 98)
CLIENT-IP: 10.2.87.142
X-FORWARDED-FOR: 10.2.87.142
Isn't Network IDS enough?

GET http://216.218.184.9/pI9Ob6SZcWQR2ODUWOopFg/81/10-2-87-142 HTTP/1.0
Connection: close
Pragma: no-cache
Accept: text/html
Host: 216.218.184.9
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; AOL 5.0; Windows 98)
CLIENT-IP: 10.2.87.142
X-FORWARDED-FOR: 10.2.87.142
Other advantages of honeypots

Advance Warning

Deployed in sufficient numbers, honeypots can generate data that can be fed into statistical models for very accurate attack prediction.

http://project.honeynet.org/papers/stats/
Other advantages of honeypots

Hearts and Minds of the Enemy
Given enough ability to interact with a compromised system, an attacker may reveal a great deal about himself.

The Honeynet Project monitored a hacking group's conversations for 4 weeks -- the group had compromised a honeypot and used it to hold an IRC channel.
Intelligence Gathering

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

--Sun Tzu, The Art of War
Intelligence Gathering

```
cd /; ls -alF; w; uname -a; id
ftp ftp.0catch.com
ls
ftp
open
ftp.0catch.com
```

```
rootkit.0catch.com
szopol
ls
passwd root
wget
```

```
# ping -f -s 65000 64.58.174.8&
# ps ax
```
Intelligence Gathering

courtesy of http://www.honeynet.org/papers

:D1ck!: wat was that IRIX box
:D1ck!: not the .edu
:D1ck!: the other one u gave me to ./own
:D1ck!: ?
:Sp07!: kcnet.org
:D1ck!: k
:D1ck!: Sp07: u have a IRIX, root kit u could send?
:Sp07!: no
:Sp07!: I just used bj
:Sp07!: the login trojan
:D1ck!: oh
:D1ck!: k
:D1ck!: send me bj.c
:D1ck!: i lost mine
Perception Management

Battlefield deception consists of those operations .... which purposely mislead enemy decision makers by--

* Distortion.
* Concealment:
* Falsification of indicators of friendly intentions, capabilities, or dispositions.

-- US Army FM-90-2
Perception Management

False banners
False TCP/IP stacks
Decoy systems
Honeynets
Perception Management
- False Banners -

Under Construction
The site you were trying to reach does not currently have a
default page. It may be in the process of being upgraded.

Please try this site again later. If you still experience the
problem, try contacting the Web site administrator.
Perception Management
- False Banners -
Perception Management
- False TCP/IP Stacks -

# wwww:ttt:mmm:D:W:S:N:I:OS Description
#
# wwww - window size
# ttt - time to live
# mmm - maximum segment size
# D  - don't fragment flag (0=unset, 1=set)
# W  - window scaling (-1=not present, other=value)
# S  - sackOK flag (0=unset, 1=set)
# N  - nop flag (0=unset, 1=set)
# I  - packet size (-1 = irrelevant)
Perception Management
- False TCP/IP Stacks -


16060:64:1460:1:0:1:1:60:Debian/Caldera Linux 2.2.x
8760:255:1380:1:0:0:0:44:Solaris 2.7
Perception Management
- False TCP/IP Stacks -
Honeypot weakness: narrow field of view

Of course, any technology has limitations. Honeypots have an extremely narrow field of view.

They only see attacks targeted directly at them.
Honeypot weakness: risk

What if an attacker takes over our honeypot and uses it to:

- Attack other systems, inside/outside our organization.
- Store and distribute contraband (illegally copied software, ...)

Honeypot weakness: detectability

If there's one or more flaws in our honeypot implementation, an attacker may be able to identify it as a honeypot!

http://www.el8.nl/p63-0x09.txt
Honeypot weakness: detectability

The attackers can download/buy the same technology that we can -- they can write and share fingerprinting tools.
Balance?

Honeypots simply add to your existing environment. They do not replace:

- Firewalls
- IDS's
- Locking down and patching systems

We can strike a balance though.
There are different types of honeypots, which mitigate whichever problem is most important to you. Let's look at them.

The first distinction we'll make is between Research and Production honeypots.
Production vs research honeypots

**Production honeypots**
Primary used to increase the immediate security of a site, through data-gathering and potentially deterrence.

**Research honeypots**
Primarily used to learn more about the black hat community's motives, methods and tools.
Production honeypots

Improve the security of a site:

• Detect attacks by being attacked, even those missed by pattern-based IDS!
• Improve the efficiency of pattern-based IDS
• Help perform incident response on production servers, since you can do thorough forensics on the honeypot even when this is impossible on production systems.
Debatable roles that production honeypots play:

- **Deception** -- provide an attacker with a platform to attack so he avoids the real servers.
- **Deterrence** -- Scare the enemy off by posting banners on the honeypot “This is a honeypot. Your activity is being logged.”
Engineering Deception

...he is skillful in defense whose opponent does not know what to attack.
--Sun Tzu, The Art of War
Engineering Deception
- Exposed Decoys -

Thanks for the intel!
Engineering Deception
- Interleaved Decoys -

DMZ

Honeypot

WWW

Honeypot

SMTP /DNS

Thanks for the intel!

Host

HP

Host

Host

HP

Host
Engineering Deception
- Lateral Decoys -

10.2.8.0/22

10.2.4.0/22
Debatable?

These roles are debatable because:

- Many attackers, especially automata, don't focus on a single system (target of choice) -- they focus on many targets of opportunity.
Research honeypots

Improve the security of the world:

• Don't directly improve the security of an organization.
• Allow us to learn about the methods, motives and tools of the black hat community.
• Sometimes instrumental in finding/understanding new worms. (Ex: Leaves, Code Red II, SQLSnake)
Which type should you use?

Most organizations should definitely start with production honeypots. They're generally simpler and fit most organizations' goals more closely.
Who uses research honeypots?

Organizations that tend to use research honeypots:

- Universities
- Government / Military
- Security researchers
- Anyone who stands to benefit from detailed threat awareness and understanding (you?)
The next feature that distinguishes one honeypot from another is the level of *interactivity*.

We'll explore this concept, then ramifications, before exploring different honeypot technologies.
Interactivity

This term reflects the range of potential interaction that an attacker can have with the honeypot.

Production honeypots are often low or medium interaction, as we'll see.
Low interactivity honeypots allow only a very limited amount and type of activity. For example, a honeypot may simply listen on every port of the machine, counting incoming communication attempts but shutting each down before any real data can be sent.
High interactivity honeypots tend to give an attacker as much room to move as possible. The most high interactivity honeypots are almost-entirely unmodified production systems, with added network components to provide monitoring and data control.
Data control

Data control refers to the process of limiting an attacker who has compromised one honeypot from launching a successful attack against another system.

This process is extremely important for limiting risk. Rather low interaction honeypots don't need us to focus on this, but most others do.
Interactivity

We'll get back to interactivity soon via examples, once we explore the issues that drive an organization towards a particular point on the interactivity scale.
Honeypots are a relatively new technology that brings a number of issues to consider:

- Legal, ethical and proprietary concerns
- Administrative overhead
- Analyst load
- Financial outlay
WARNING: I'm not a lawyer. I cannot tell you whether your honeypot technology and policy is legal in your region, state or country. You should consult local counsel before deploying any of this technology.
Legal concerns: who do we ask?

The Honeynet Project talks to Richard Salgado, a prosecutor in the Computer Crime and Intellectual Property Section of the US Department of Justice, who specializes in investigating and prosecuting computer network intrusions and attacks.

We can't even try to paraphrase him here.
What should you ask your lawyer?

You might ask your lawyer about the following laws and how they apply:

• Federal Wiretap Act
• Pen Register/Trap and Trace Statute
• Electronic Communication Privacy Act
• US Patriot Act
• State and local legislation and opinions
The kinds of questions people have

- Is it legal to monitor an intruder on my network or system or does he have a right to privacy?
- Is it legal to monitor an intruder's communications via the honeypot, even when the other parties in that communication are not intruders or consenters to that monitoring?
- What are the legal ramifications of an attacker using my honeypot to compromise other systems?
Ethical Concerns: privacy

The ethical concerns, again, center around questions of privacy and become difficult when one remembers that other parties to the communications that you're monitoring may not be black hats and/or may not know that they're speaking in the presence of (or via) a compromised system.
Ethical Concerns: harm

The other ethical concern has to do with whether you make it easier for an attacker to compromise someone else through your machine by putting that machine out on the network to be compromised.
Administrative/Analyst load

Honeypots can require a great deal of care and feeding, depending on how they're designed.

High interactivity honeypots, in particular, require monitoring and maintenance by someone who understands the honeypot operating system.

You can mitigate this by using a commercial honeypot with a support contract. Unfortunately, that ties you to commercial solutions.
Hardware isn't usually expensive for honeypots. Unlike firewalls and IDS's, honeypot technology doesn't demand the fastest in processors, hard drives and memory.

The costs in honeypots come down to software, if you're buying commercial, and employee time, regardless of type.
Honeypot technologies

Let's start talking about the different honeypots:
• Null listeners
• Service emulation
• System emulation
• Restricted environment
• Live computer
• Virtual machines
• Honeynet
Null listeners

Null listeners are simple programs that listen on one or more set ports for incoming connections. They receive some amount of data, generally providing little/none in return and usually allow the client to close the connection off.

```
nc -L -p 17300 >> c:\temp\kuang2.cap
```
Null listeners: evaluation

Interactivity: Low

Usefulness: Good for trend analysis and when you might be attacked, if deployed properly.

Risk: Very low risk, as there's an extremely low probability that a null-listener machine will be compromised.
Service emulations

Service emulators listen on a set of ports, just like the null listeners. The difference is that they'll try to look like the normal program that would talk on that port. These differ in how thorough they are -- some just pop up a header for the service, but don't make any other replies. Others accurately mimic the behavior of a particular program on a particular operating system.
Service emulations: evaluation

Interactivity: Medium

Usefulness: Good for trend analysis and for spotting some automated tools/worms

Risk: Fairly low risk, as there's a low probability that the program will be compromised. It's still usually somewhat simple, in that it doesn't grant an attacker a diverse range of access.
Host / Service Emulators

• Back Officer Friendly
  - Back Orifice emulator
  - very thin telnet & ftp emulators
• Deception Toolkit
  - Series of compiled responders
  - DTK port 365
• Verizon NetFacade
  - Up to 255 addresses & 14 services
  - HTTP redirection to live hosts
  - target stack emulation - fools nmap & cheops
Example: Specter

Specter was created by NetSec, with functionality like an enterprise version of BOF. Includes service emulation for 7 protocols, null listeners for 7 more ports, 6 of which must be predefined. Will change banners to match one of 13 different operating system. Only affects the application layer -- someone fingerprinting the machine could tell that it wasn't the right O/S.
Specter has “characters”

- Open -- simulates vulnerabilities on the system, like open mail relaying
- Secure -- simulates a hardened or patched system
- Aggressive -- tries to scare off the attacker with warnings
- Failing -- acts like a broken machine to confuse and delay an attacker
- Random -- chooses a different character for every connection
Your actions are logged, intrusion alert was activated.
<table>
<thead>
<tr>
<th>Type</th>
<th>Time</th>
<th>Source IP</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>2001/10/09 14:26:54</td>
<td>192.168.1.244 [iris.lab3.netsec.ch]</td>
<td>SMTP-20011009-142654.txt</td>
</tr>
<tr>
<td>TELNET</td>
<td>2001/10/28 15:40:05</td>
<td>199.224.86.36 [thyme.epix.net]</td>
<td>TELNET-20011028-154005.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/10/29 17:35:07</td>
<td>195.184.228.217 [d8-228-217-dial.mistral.co.uk]</td>
<td>HTTP-20011029-173507.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/10/29 08:36:06</td>
<td>195.47.152.55 [p307-055.ppp.get2net.dk]</td>
<td>HTTP-20011029-083606.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/10/29 08:36:07</td>
<td>195.47.152.55 [p307-055.ppp.get2net.dk]</td>
<td>HTTP-20011029-083607.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/10/29 08:36:16</td>
<td>195.47.152.55 [p307-055.ppp.get2net.dk]</td>
<td>HTTP-20011029-083616.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/10/29 08:36:17</td>
<td>195.47.152.55 [p307-055.ppp.get2net.dk]</td>
<td>HTTP-20011029-083617.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/11/02 16:04:26</td>
<td>195.130.92.207 [gserver.telkav.edu.gr]</td>
<td>HTTP-20011102-160426.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/11/03 01:52:26</td>
<td>195.55.104.64 [zacky.arrouada.net]</td>
<td>HTTP-20011103-015226.txt</td>
</tr>
<tr>
<td>HTTP</td>
<td>2001/11/03 01:52:46</td>
<td>195.55.104.64 [zacky.arrouada.net]</td>
<td>HTTP-20011103-015246.txt</td>
</tr>
<tr>
<td>FTP</td>
<td>2001/11/03 05:16:42</td>
<td>212.185.235.84 [p489e854.dip.t-dialin.net]</td>
<td>FTP-20011103-051642.txt</td>
</tr>
<tr>
<td>TELNET</td>
<td>2001/11/03 06:02:47</td>
<td>80.65.225.80 [vega.lab6.netsec.ch]</td>
<td>TELNET-20011103-060247.txt</td>
</tr>
<tr>
<td>POP3</td>
<td>2002/01/11 03:04:23</td>
<td>192.168.3.17 [vega.lab6.netsec.ch]</td>
<td>POP3-20020111-030423.txt</td>
</tr>
</tbody>
</table>
Example: Tiny Honeypot

• Tiny Honeypot (thp) is an Open Source low-interaction honeypot written in Perl.
• Runs on a network firewall, or individual host
• Provides “Ubiquitous Redirection” whereas every connection succeeds, regardless of target port or address.
• thp has plugins for FTP and HTTP, providing strong emulations for these protocols, and is easily extended.
Example: Tiny Honeypot

- thp can listen for RPC connections to the portmapper and log the output, using hooks left by Wietese Venema in his portmapper rewrite.
- does not change the non-application behavior of the system:
- thp might show a Windows service on a port, while nmap's OS detection will find that the machine is running Linux.
Example: Tiny Honeypot

Apr 15 17:54:38 SID=407F049E445CA.shell PID=11339 SRC=200.184.8.79 SPT=1425 ET=00:00:05
BYTES=59
NICK klux
USER hyper "kolti.net" "10.129.154.3" :7
QUIT :

Apr 15 17:54:51 SID=407F04AB1605B.shell PID=11383 SRC=200.145.158.176 SPT=1061 ET=00:00:28
BYTES=41
uname -0a
uname -a
ifco
exit

Apr 15 17:54:54 SID=407F04AEA9F5.shell PID=11389 SRC=201.3.141.218 SPT=50136 ET=00:00:28
BYTES=24
SUCK MY EGGS ADMIN

Apr 15 17:55:18 SID=407F04C67C926.shell PID=11414 SRC=62.248.102.74 SPT=52155 ET=00:00:14
BYTES=48
ps x
cd /tmp
Example: Honeyd

Honeyd is a low-interaction honeypot that provides service emulation, null listeners and actually will change the behavior of the TCP/IP stack to make the system appear to be any other system in the nmap signatures database. Like thp, honeyd provides service emulation through plugins.
Honeyd does have a nice trick. It can listen on a LAN for probes or attacks to systems that aren't in its ARP table. After sending its own ARP request out for one of these missing systems, it will ARP-spoof to answer for any unclaimed IP addresses that are being probed.

thp and honeyd can both grab an entire netblock full of addresses, as large as you want.
Live Computer

The simplest form of honeypot is a live computer, unmodified.

The risk, though, is way too high unless you can add a data control device to prevent an attacker from doing damage from that live system.
Live Computer: Evaluation

Interactivity: Extremely high. An attacker can do absolutely anything he could do to a normal compromised system.

Usefulness: High. There's a good deal of data to be had if you can figure out how to get it.

Risk: Extremely high. An attacker can potentially launch attacks from the compromised system.
Virtual Machines

In the virtual machine model, you run a guest operating system as a child of an existing system. The host operating system generally can gather a great deal of data about what's trying to attack from/against the guest. You can build this functionality with VMware or User Mode Linux, but it's also available via Symantec's Decoy Server aka Recourse ManTrap.
Virtual Machine: Evaluation

Interactivity: Very high. An attacker can do nearly anything he could do to a normal compromised system.

Usefulness: High. There's a good deal of data to be had if you can figure out how to get it.

Risk: High. An attacker can potentially launch attacks from the guest system unless the host has data controls configured.
Example: Symantec Decoy Server

• Symantec's Decoy Server, originally Recourse Mantrap, runs on a Solaris system and creates up to 4 “cages,” or virtual machines identical to the host operating system.
• Each of these machines can be attacked, with Decoy Server keeping excellent logs of exactly what's going on with those systems.
• Java management console runs on any machine with a JRE 1.4+
• Provides trend charts & graphs
Honeynet

The honeynet is a special type of honeypot. It's a network whose purpose is to be probed, attacked and compromised. It can have one or more honeypots, but it must have facilities for both data control and data capture.

Data capture -- obtaining all data possible about an attack
Data control -- restricting a compromised honeypot from attacking other organizations' hosts.
Honeynet: Evaluation

Interactivity: High -- each of the machines in the network is a live system honeypot.
Usefulness: High -- this construct is currently the most risky available while still maintaining some data control, second only to raw live systems.
Risk: Medium-High -- risk is well-mitigated by the extensive data control utilities in use.
Virtual honeynet with VMware/UML

• Though VMware isn't designed for this, we can use VMware to get nearly the same functionality as Decoy Server, without the kernel-level logging.
• VMware lets you run an Intel box in a window and simulates that system down the hardware level. The risk is about as high as in a normal honeynet.
• Usermode Linux honeypot extensions provide jail operation, kernel syscall logging, tty logging, etc.
A HONEYNET is a NETWORK whose entire value lies in being attacked.

Every packet is logged because...

...every packet is suspicious.
Generation I Honeynet Diagram
Where Do You Put A Honeynet?

This is the same issue that occurs with the Intrusion Detection System (IDS).

If you place the IDS outside of the firewall...  
...you get all attacks, including those that wouldn't have worked.

If you place the IDS inside the firewall...  
...you miss activity.
Where Do We Put Our Honeynets?

While our honeynets include a firewall, we generally allow all traffic from the Internet to reach the honeypots.

We want all of the data that we can get! That's because we're using this for research.
Research Honeypots/Honeynets vs. Production Honeypots/Honeynets?

Most corporations tend to use production honeypots, which usually mirror existing production systems.

The goals of these honeypots are to:
- Determine how those systems can/will be attacked: vulnerability assessment
- Provide the corporation with an early warning of attacks
Research organizations, like .edu, .mil and the Honeynet project tend to use research honeypots to learn as much as possible.

This is time intensive!
It also produces the most information about new threats.
Placement of The Honeynet

You can place your honeynet wherever you like, based on:

- How much information you want
- How tailored you want this to be to your environment
Risks

The risks associated with honeynets are that:

• The attacker can use your system to attack others
• The attacker may realize that he has taken over a honeypot
Big Risk: Your Systems are used to Attack Others

We do a great deal to lessen this risk:

• We don't allow any ICMP out of the honeynet AT ALL!!
• We limit the number of new connections that any honeypot can make 5-10 or 5-10 per hour
• We configure the firewall to alert us to ANY outgoing connections, usually by paging us
Honeynet Generation II 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 layer 2 (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 administration.
- **Interface A**: Layer 2 interface segmenting production network.
- **Interface B**: Layer 2 interface segmenting Honeynet network.
- **Interface C**: Layer 3 interface VPN connection to collection point.
ISTS Distributed Honeypot Project

Funded by DHS - ODP
Seeks to -
codify honeypot technology selection criteria
trend attacker behavior
rate attacker skills & effectiveness of deceptions
ISTS Distributed Honeypot Project

GENII single & dual virtual host honeynets
Central database and administrative management
Participants include:
isps
security research sites
defense contractors
academia
individuals
Risk Mitigating Steps

Read Honeynet Project white papers
   http://www.honeynet.org
Evaluate and deploy appropriate deception technologies.
Audit deception systems regularly
   share and apply lessons learned
   IDS rules, firewall rules, awareness briefings
Participate in a community effort & benefit from aggregate analysis that is
directly relevant!
Q & A
Honeypots and the Enterprise: Intelligence-based Risk Management

Institute for Security Technology Studies
Dartmouth College
Hanover, New Hampshire

George Bakos - gbakos@ists.dartmouth.edu