Honeypots

The Future
Your Speaker

- Founder, Honeynet Project & Moderator, honeypot mailing list
- Author, *Honeypots: Tracking Hackers & Co-author, Know Your Enemy*
- Officer, Rapid Deployment Force
- Worked with CIA, NSA, FBI, DOJ, President’s Advisory Board, Army, Navy
Purpose

Latest developments with honeypots.
Agenda

- Honeypots
- Low Interaction
- High Interaction
Honeypots
Problem

- Your resources are a big, fat static target. The bad guys can attack them whenever they want, however they want.

- The bad guys have the initiative (and are getting better).
New Tactics - Backdoor
IPv6 Tunneling

<table>
<thead>
<tr>
<th>Date: 12/01-18:13:11</th>
<th>Source: 163.162.170.173</th>
<th>Destination: 192.168.100.28</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 TTL: 11</td>
<td>TOS: 0x00</td>
<td>ID: 33818</td>
</tr>
<tr>
<td>IpLen: 20</td>
<td>DgmLen: 1124</td>
<td></td>
</tr>
<tr>
<td>60 00 00 00 04 28 06 3B 20 01 07 50 00 02 00 00</td>
<td><code>.....(; ..P.....</code></td>
<td></td>
</tr>
<tr>
<td>02 02 A5 FF FE F0 AA C7 20 01 06 B8 00 00 04 00</td>
<td><code>......... ........</code></td>
<td></td>
</tr>
<tr>
<td>00 00 00 00 00 00 5D 0E 1A 0B 80 0C AB CF 0A 93</td>
<td><code>........] ........</code></td>
<td></td>
</tr>
<tr>
<td>03 30 B2 C1 50 18 16 80 C9 9A 00 00 3A 69 72 63</td>
<td><code>.0..P.........:irc</code></td>
<td></td>
</tr>
<tr>
<td>36 2E 65 64 69 73 6F 6E 74 65 6C 2E 69 74 20 30</td>
<td>6.edisontel.it 01 <code>OwnZ`` :Welc</code></td>
<td></td>
</tr>
<tr>
<td>30 31 20 60 4F 77 6E 5A 60 60 20 3A 57 65 6C 63</td>
<td><code>net Relay Networ</code></td>
<td></td>
</tr>
<tr>
<td>6F 6D 65 20 74 6F 70 74 68 65 20 49 6E 74 65 72</td>
<td>k <code>OwnZ``!~ahaa@</code></td>
<td></td>
</tr>
<tr>
<td>6E 65 74 20 52 65 6C 61 79 20 4E 65 74 77 6F 72</td>
<td>bacardi.orange.o`</td>
<td></td>
</tr>
<tr>
<td>6B 20 60 4F 77 6E 5A 60 60 21 7E 61 68 61 61 40</td>
<td>rg.ru...:irc6.edi`</td>
<td></td>
</tr>
<tr>
<td>62 61 63 61 72 64 69 2E 6F 72 61 6E 67 65 2E 6F</td>
<td>sontel.it 002 <code>O</code></td>
<td></td>
</tr>
<tr>
<td>72 67 2E 72 75 0D 0A 3A 69 72 63 3E 2E 65 64 69</td>
<td>wnZ``:Your host`</td>
<td></td>
</tr>
<tr>
<td>73 6F 6E 74 65 6C 2E 69 74 20 30 30 32 20 60 4F</td>
<td>is irc6.edisont</td>
<td></td>
</tr>
</tbody>
</table>
Solution

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

A security resource who’s value lies in being probed, attacked, or compromised.
The Concept

- System has no production value, no authorized activity. Theoretically they should see nothing.

- 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 many different applications to security.
Types of Honeypots

- Interaction measures the activity a honeypot allows the attacker.

- The more interaction you allow, the more you can learn.

- The more interaction you allow, the complexity and risk you have.
Low interaction honeypots

- Primarily emulate services and operating systems.

- Emulation is easier to deploy and contains the attackers' activity.

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

High-interaction honeypots

- Used to gain information. That information has different value to different organizations.

- Does not emulate, but runs actual operating systems. Install FTP server.
<table>
<thead>
<tr>
<th>Host Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cage 1</td>
</tr>
<tr>
<td>Cage 2</td>
</tr>
<tr>
<td>Cage 3</td>
</tr>
<tr>
<td>Cage 4</td>
</tr>
</tbody>
</table>
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)
Advances in Low-Interaction
Example - Honeyd honeypot

- OpenSource honeypot developed by Niels Provos.
- Production honeypot.
- Emulates services and operating systems.
How Honeyd works

- Monitors unused IP space.
- When it sees connection attempt, assumes IP and interacts with attacks.
- Can monitor literally millions of IP addresses at the same time.
Network with unused IPs
Monitors unused IPs
Capabilities

- Emulate IP stacks
- Create fake networks with latency
- Emulates advanced services
- Create dynamic IDS signatures
NetBait

- Not a product, a service.
- Attackers directed to honeypot pool, which can be located in a different, isolated network.
Real Network
Attacker Sees
Hot Zoning

Valid inbound SMTP traffic

All inbound non TCP 25 traffic OR any SMTP based attacks

Mailserver

Honeynet Gateway

Target System
Smoke Detector

Before

After
Honeytokens

- Resources used for detection and tracking attackers.
- Items that should not be used.
  - Fake patient records
  - Bogus SSN or CC numbers
  - Planted files or documents (ala Cuckoo’s Egg)
High Interaction Technology
Honeynets

- Honeynets are a high-interaction honeypot.
- Not a product, but an architecture.
- An entire network of systems designed to be compromised.
Latest Developments

- Snort_Inline
- Sebek2
- Bootable CDROM
- User Interface
GenII Honeynet
drop tcp $EXTERNAL_NET any -> $HOME_NET 53
(msg:"DNS EXPLOIT named";flags: A+;
content:"|CD80 E8D7 FFFFFFFF|/bin/sh";

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

Snort-inline
Sebek2

- Capture bad guys activities without them knowing.
- Insert kernel mods on honeypots.
- Mods are hidden
- Dump all activity to wire
- Bad guy can sniff any packet with pre-set MAC
Sebek2 Configuration

#----- sets destination IP for sebek packets
DESTINATION_IP="192.168.1.254"

#----- sets destination MAC addr for sebek packets
DESTINATION_MAC="00:01:C9:F6:D3:59"

#----- defines the destination udp port sebek sends to
DESTINATION_PORT=34557

#----- controls what SRC MAC OUIs to hide from users
FILTER_OUI="0A:0B:0C"
Sebek2 Output

06:06:25-2003/03/23 [0:mingetty:6785:vc/1:0]
06:06:26-2003/03/23 [0:mingetty:6785:vc/1:0] root
06:06:50-2003/03/23 [0:bash:13674:vc/1:0] ifconfig -a
06:06:58-2003/03/23 [0:bash:13674:vc/1:0] exec csh
06:07:12-2003/03/23 [0:ftp:13738:vc/1:0] lbye
06:07:19-2003/03/23 [0:csh:13674:vc/1:16] vi /etc/resolv.conf
06:07:22-2003/03/23 [0:vim:13739:vc/1:0] 1:q
06:09:39-2003/03/23 [0:csh:13674:vc/1:16]
Bootable CDROM

- Insert CDROM
- Boot
- Instant Honeynet Gateway (Honeywall)
User Interface

- Runs on Honeywall
- Analyze attacks in real time

Demo
<table>
<thead>
<tr>
<th>Date - Time</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003-01-18 15:42:16</td>
<td>TCP</td>
<td>202.107.52.170</td>
<td>34781</td>
<td>10.1.1.105</td>
<td>21</td>
<td>view, p0f, ARIN (100)</td>
</tr>
<tr>
<td>2003-01-18 15:45:18</td>
<td>TCP</td>
<td>202.107.52.170</td>
<td>53763</td>
<td>10.1.1.103</td>
<td>21</td>
<td>view, p0f, ARIN (651)</td>
</tr>
<tr>
<td>2003-01-18 15:45:18</td>
<td>TCP</td>
<td>202.107.52.170</td>
<td>53764</td>
<td>10.1.1.101</td>
<td>21</td>
<td>view, p0f, ARIN (604)</td>
</tr>
<tr>
<td>2003-01-18 15:45:18</td>
<td>TCP</td>
<td>10.1.1.101</td>
<td>1027</td>
<td>202.107.52.170</td>
<td>113</td>
<td>view, ARIN (100)</td>
</tr>
<tr>
<td>2003-01-18 15:47:04</td>
<td>TCP</td>
<td>202.107.52.170</td>
<td>53996</td>
<td>10.1.1.101</td>
<td>21</td>
<td>view, p0f, ARIN, Snort (15k)</td>
</tr>
<tr>
<td>2003-01-18 15:47:05</td>
<td>TCP</td>
<td>10.1.1.101</td>
<td>1028</td>
<td>202.107.52.170</td>
<td>113</td>
<td>view, ARIN (100)</td>
</tr>
<tr>
<td>2003-01-18 15:50:42</td>
<td>TCP</td>
<td>10.1.1.101</td>
<td>1029</td>
<td>202.107.52.170</td>
<td>113</td>
<td>view, ARIN (100)</td>
</tr>
<tr>
<td>2003-01-18 15:52:16</td>
<td>TCP</td>
<td>62.99.207.73</td>
<td>3068</td>
<td>10.1.1.101</td>
<td>80</td>
<td>view, p0f, ARIN, plugin (9k)</td>
</tr>
<tr>
<td>2003-01-18 15:53:28</td>
<td>TCP</td>
<td>202.162.193.147</td>
<td>61115</td>
<td>10.1.1.101</td>
<td>22</td>
<td>view, p0f, ARIN (55k)</td>
</tr>
<tr>
<td>2003-01-18 15:54:46</td>
<td>TCP</td>
<td>10.1.1.101</td>
<td>1030</td>
<td>212.15.64.41</td>
<td>80</td>
<td>view, ARIN, plugin (522k)</td>
</tr>
<tr>
<td>2003-01-18 15:54:46</td>
<td>ICMP</td>
<td>10.14.0.20</td>
<td>0</td>
<td>10.1.1.101</td>
<td>0</td>
<td>view, ARIN (0)</td>
</tr>
<tr>
<td>2003-01-18 15:55:37</td>
<td>ICMP</td>
<td>10.14.0.20</td>
<td>0</td>
<td>10.1.1.101</td>
<td>0</td>
<td>view, ARIN (0)</td>
</tr>
<tr>
<td>2003-01-18 15:56:34</td>
<td>TCP</td>
<td>10.1.1.101</td>
<td>1031</td>
<td>205.158.62.27</td>
<td>25</td>
<td>view, ARIN (1k)</td>
</tr>
<tr>
<td>2003-01-18 15:57:35</td>
<td>UDP</td>
<td>64.56.227.36</td>
<td>1026</td>
<td>10.1.1.101</td>
<td>137</td>
<td>view, ARIN (78)</td>
</tr>
<tr>
<td>2003-01-18 15:57:35</td>
<td>UDP</td>
<td>64.56.227.36</td>
<td>1026</td>
<td>10.1.1.103</td>
<td>137</td>
<td>view, ARIN (78)</td>
</tr>
<tr>
<td>2003-01-18 15:57:35</td>
<td>UDP</td>
<td>64.56.227.36</td>
<td>1026</td>
<td>10.1.1.104</td>
<td>137</td>
<td>view, ARIN (78)</td>
</tr>
</tbody>
</table>
Summary

- We are just beginning to see the potential for honeypots.

- Honeypots are where firewalls were ten years ago (Marcus Ranum)
Resources

- Honeypot website
  - www.tracking-hackers.com

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

- *Know Your Enemy*
  - www.honeynet.org/book/

- *Honeypots: Tracking Hackers*
Contact

Lance Spitzner
<lance@honeynet.org>