Getting back at Trudy

SSH Botnet Member Credential Collection using Connect Back Honeypots

Tobias Fiebig

University of Amsterdam

01/08/2013
• SSH-Bruteforcing.

• Systems on the internet trying to authenticate to your system with all kinds of stupid usernames and passwords.
• Ok? Who had the problem of being owned by an SSH-Bruteforcer?
Ok, hands up...

• Ok? Who had the problem of being owned by an SSH-Bruteforcer?

• Ok, lets ask differently... Who knows somebody who has a friend whose father in law’s dog once had this problem... ?
Getting back at Trudy

Tobias Fiebig

Introduction
SSH-Bruteforce Attacks
The Idea
Ethical Implications
Legal Implications

The Software
What it is... How it works...

Experiments
Single Hosts Whole Networks

Results
Single Hosts Whole Networks Something funny...

Conclusion

Honestly... hit me as well...

From: Intrusion Detection Team <idt@******navy.mil>
To: abuse@wybt.net
Subject: hacker activity 195.191.196:...
Date: [Redacted]

This email is for your information. It is *not* a request for any specific action. It was automatically generated, but all replies will be handled personally.

A host/port sweep

TCP Port 22 Sweep of OUR subnet(s):

FROM 195.191.196 [wybt.net [DE]]
Starttime [Redacted]; Endtime [Redacted]
TCP Port 22: attempts on about 76 addresses.

was logged at this United States Department of Defense facility, apparently originating from one of your machines. The time zone is POT (Greenwich -7 hours).

Suggested interpretations:
1. One of your machines has been compromised/infected and is scanning our networks.
2. One of your users is scanning our networks.

Thank you for your attention.

--Intrusion Detection Team
idt@******navy.mil
Where do these systems come from?

• Probably not the attackers homebox...
• But what kind of system could such an attacker have at his disposal?
• Yes, systems they penetrated by Bruteforcing the SSH daemon...
Where do these systems come from?

- Probably not the attackers homebox...
Where do these systems come from?

- Probably not the attackers homebox...
- But what kind of system could such an attacker have at his disposal?
Where do these systems come from?

• Probably not the attackers homebox…
• But what kind of system could such an attacker have at his disposal?
• Yes, systems they penetrated by Bruteforcing the SSH daemon…
What do we know about these systems?

- You get detected if you change the password.
- The password that is used, is probably in the attacker's wordlist.
- The attacker runs his SSH Bruteforcing Software on that machine.
- Wait... what?
What do we know about these systems?

- You get detected if you change the password.
What do we know about these systems?

- You get detected if you change the password.
- The password that is used, is probably in the attackers wordlist.
What do we know about these systems?

- You get detected if you change the password.
- The password that is used, is probably in the attackers wordlist.
- The attacker runs his SSH Brute forcing Software on that machine.
What do we know about these systems?

- You get detected if you change the password.
- The password that is used, is probably in the attackers wordlist.
- The attacker runs his SSH Bruteforcing Software on that machine.
- Wait... what?
Research Question: Does this work?

1. SSH Connection Attempt from Bruteforcer to Honeypot
   - User: root
   - Password: 123456

2. SSH Connection Attempt from Honeypot to Bruteforcer
   - User: root
   - Password: 123456

3. Bruteforcer returns auth Result

4. Honeypot returns auth Denied
• Subjects may be unaware of infection/participation in the research.
Ethical Implications

- Subjects may be unaware of infection/participation in the research.
  - Inform subjects. Has been done via appropriate channels.
• Subjects may be unaware of infection/participation in the research.
  • Inform subjects. Has been done via appropriate channels.
• Gathered data is pretty sensitive.
Ethical Implications

• Subjects may be unaware of infection/participation in the research.
  • Inform subjects. Has been done via appropriate channels.
• Gathered data is pretty sensitive.
  • Fully anonymize data before publication.
Legal Implications

• Different jurisdictions touched.
• In nearly all cases: Unauthorized logins prohibited by applicable law.
Legal Implications

- Different jurisdictions touched.
- In nearly all cases: Unauthorized logins prohibited by applicable law.
  → Do not login, just authenticate.
Getting back at Trudy

Tobias Fiebig

Introduction
SSH-Bruteforce Attacks
The Idea
Ethical Implications
Legal Implications

The Software
What it is...
How it works...

Experiments
Single Hosts
Whole Networks

Results
Single Hosts
Whole Networks
Something funny...

Conclusion

Just quickly thrown together...

• Something that can:
Just quickly thrown together...

• Something that can:‘
  • Provide an SSH server.
• Something that can:‘
  • Provide an SSH server.
  • Get Username/Password combinations
• Something that can:
  • Provide an SSH server.
  • Get Username/Password combinations
  • Try to authenticate to the remote SSH server, without opening a session.
Paramiko to the Rescue!

- Based on the Open Source python ssh library paramiko\(^1\) and the demo SSH server provided with it.
- Patched for threading, multiple simultaneous connections, providing an Ubuntu 12.04-style banner and the connect-back feature.
- Basically: 165 lines of python code after patching.

\(^1\)http://www.lag.net/paramiko/
Just with a few hosts...

- 8 Hosts
- 4 Countries, Two Continents, 8 AS
- All systems listened with the sshcb software on port 22
- Ran for appr. 2 weeks
... and with some /24s.

- 8 /24 subnets from different /16
  - 6 from RIPE as temporary assignment
  - 1 from SNE/SURFnet
  - 1 from WYBT.net

- Each networks port 22 and ICMP DNATed to one box listening with the sshcb software on port 22

- Also ran for appr. 2 weeks
# Single Host Study

<table>
<thead>
<tr>
<th>Host</th>
<th>Avg. Connections/h</th>
<th>Max Connections/h</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>232.06</td>
<td>3063</td>
<td>69386</td>
</tr>
<tr>
<td>p2o1</td>
<td>26.96</td>
<td>1136</td>
<td>8062</td>
</tr>
<tr>
<td>p2o2</td>
<td>18.46</td>
<td>746</td>
<td>5519</td>
</tr>
<tr>
<td>p2o3</td>
<td>24.97</td>
<td>1219</td>
<td>7467</td>
</tr>
<tr>
<td>p2o4</td>
<td>19.68</td>
<td>645</td>
<td>5886</td>
</tr>
<tr>
<td>p2o5</td>
<td>25.81</td>
<td>793</td>
<td>7716</td>
</tr>
<tr>
<td>p2o6</td>
<td>41.40</td>
<td>1560</td>
<td>12379</td>
</tr>
<tr>
<td>p2o7</td>
<td>35.11</td>
<td>717</td>
<td>10497</td>
</tr>
<tr>
<td>p2o8</td>
<td>39.67</td>
<td>3042</td>
<td>11860</td>
</tr>
</tbody>
</table>

Table: Base Data for Single Host Study
Single Host Study

<table>
<thead>
<tr>
<th>Host</th>
<th>Penetrated Hosts</th>
<th>Non Penetrated Hosts</th>
<th>Successrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>30</td>
<td>290</td>
<td>9.38%</td>
</tr>
<tr>
<td>p2o1</td>
<td>2</td>
<td>49</td>
<td>3.92%</td>
</tr>
<tr>
<td>p2o2</td>
<td>8</td>
<td>65</td>
<td>10.96%</td>
</tr>
<tr>
<td>p2o3</td>
<td>1</td>
<td>42</td>
<td>2.33%</td>
</tr>
<tr>
<td>p2o4</td>
<td>1</td>
<td>37</td>
<td>2.63%</td>
</tr>
<tr>
<td>p2o5</td>
<td>4</td>
<td>43</td>
<td>8.51%</td>
</tr>
<tr>
<td>p2o6</td>
<td>6</td>
<td>53</td>
<td>10.17%</td>
</tr>
<tr>
<td>p2o7</td>
<td>4</td>
<td>58</td>
<td>6.45%</td>
</tr>
<tr>
<td>p2o8</td>
<td>4</td>
<td>36</td>
<td>10.00%</td>
</tr>
</tbody>
</table>

Table: Success Rate for Single Host Study
# Network Study

<table>
<thead>
<tr>
<th>Net</th>
<th>Avg. Connections/h</th>
<th>Max Connections/h</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>1993.72</td>
<td>33027</td>
<td>663912</td>
</tr>
<tr>
<td>145.100.109.0/24</td>
<td>668.87</td>
<td>25202</td>
<td>222736</td>
</tr>
<tr>
<td>151.216.20.0/24</td>
<td>182.19</td>
<td>3598</td>
<td>60670</td>
</tr>
<tr>
<td>151.217.0.0/24</td>
<td>173.47</td>
<td>8294</td>
<td>57767</td>
</tr>
<tr>
<td>151.220.0.0/24</td>
<td>211.29</td>
<td>8186</td>
<td>70361</td>
</tr>
<tr>
<td>151.221.0.0/24</td>
<td>192.38</td>
<td>8218</td>
<td>64064</td>
</tr>
<tr>
<td>151.222.0.0/24</td>
<td>175.58</td>
<td>3740</td>
<td>58470</td>
</tr>
<tr>
<td>151.223.0.0/24</td>
<td>196.59</td>
<td>8296</td>
<td>65466</td>
</tr>
<tr>
<td>195.191.197.0/24</td>
<td>193.32</td>
<td>3468</td>
<td>64378</td>
</tr>
</tbody>
</table>

Table: Base Data for Network Study
Network Study

<table>
<thead>
<tr>
<th>Net</th>
<th>Penetrated Hosts</th>
<th>Non Penetrated Hosts</th>
<th>Successrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>36</td>
<td>632</td>
<td>5.38%</td>
</tr>
<tr>
<td>145.100.109.0/24</td>
<td>14</td>
<td>74</td>
<td>15.91%</td>
</tr>
<tr>
<td>151.216.20.0/24</td>
<td>13</td>
<td>257</td>
<td>4.81%</td>
</tr>
<tr>
<td>151.217.0.0/24</td>
<td>11</td>
<td>180</td>
<td>5.76%</td>
</tr>
<tr>
<td>151.220.0.0/24</td>
<td>12</td>
<td>287</td>
<td>4.01%</td>
</tr>
<tr>
<td>151.221.0.0/24</td>
<td>8</td>
<td>202</td>
<td>3.81%</td>
</tr>
<tr>
<td>151.222.0.0/24</td>
<td>9</td>
<td>193</td>
<td>4.46%</td>
</tr>
<tr>
<td>151.223.0.0/24</td>
<td>8</td>
<td>201</td>
<td>3.83%</td>
</tr>
<tr>
<td>195.191.197.0/24</td>
<td>4</td>
<td>158</td>
<td>2.47%</td>
</tr>
</tbody>
</table>

Table: Success Rate for Network Study
Getting back at Trudy

Tobias Fiebig

Introduction
SSH-Bruteforce Attacks
The Idea
Ethical Implications
Legal Implications

The Software
What it is...
How it works...

Experiments
Single Hosts
Whole Networks

Results
Single Hosts
Whole Networks
Something funny...

Conclusion
### Network Study

**Table: Base Data for Network Study - outliers filtered**

<table>
<thead>
<tr>
<th>Net</th>
<th>Avg. Connections/h</th>
<th>Max Connections/h</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>1732.44</td>
<td>33027</td>
<td>576901</td>
</tr>
<tr>
<td>145.100.109.0/24</td>
<td>668.88</td>
<td>25202</td>
<td>222736</td>
</tr>
<tr>
<td>151.216.20.0/24</td>
<td>140.88</td>
<td>3598</td>
<td>46913</td>
</tr>
<tr>
<td>151.217.0.0/24</td>
<td>136.90</td>
<td>8294</td>
<td>45587</td>
</tr>
<tr>
<td>151.220.0.0/24</td>
<td>176.31</td>
<td>8186</td>
<td>58710</td>
</tr>
<tr>
<td>151.221.0.0/24</td>
<td>161.26</td>
<td>8218</td>
<td>53698</td>
</tr>
<tr>
<td>151.222.0.0/24</td>
<td>135.40</td>
<td>3696</td>
<td>45089</td>
</tr>
<tr>
<td>151.223.0.0/24</td>
<td>156.77</td>
<td>8296</td>
<td>52204</td>
</tr>
<tr>
<td>195.191.197.0/24</td>
<td>156.05</td>
<td>3468</td>
<td>51964</td>
</tr>
</tbody>
</table>
Network Study

<table>
<thead>
<tr>
<th>Net</th>
<th>Penetrated Hosts</th>
<th>Non Penetrated Hosts</th>
<th>Successrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>35</td>
<td>260</td>
<td>11.86%</td>
</tr>
<tr>
<td>145.100.109.0/24</td>
<td>14</td>
<td>74</td>
<td>15.91%</td>
</tr>
<tr>
<td>151.216.20.0/24</td>
<td>12</td>
<td>148</td>
<td>7.50%</td>
</tr>
<tr>
<td>151.217.0.0/24</td>
<td>10</td>
<td>83</td>
<td>10.75%</td>
</tr>
<tr>
<td>151.220.0.0/24</td>
<td>11</td>
<td>93</td>
<td>10.58%</td>
</tr>
<tr>
<td>151.221.0.0/24</td>
<td>7</td>
<td>93</td>
<td>7.00%</td>
</tr>
<tr>
<td>151.222.0.0/24</td>
<td>8</td>
<td>89</td>
<td>8.25%</td>
</tr>
<tr>
<td>151.223.0.0/24</td>
<td>7</td>
<td>85</td>
<td>7.61%</td>
</tr>
<tr>
<td>195.191.197.0/24</td>
<td>4</td>
<td>113</td>
<td>3.42%</td>
</tr>
</tbody>
</table>

Table: Success Rate for Network Study - outliers filtered
• Some passwords are not like other passwords. They are special.
Uncovered group passwords...

- Some passwords are not like other passwords. They are special.
- Example: “spargeosu#%^%*&138cucapulinpicior”
Some passwords are not like other passwords. They are special.

Example: “spargeosu#$%^*&138cucapulinpicior”

Successfull connect back attempts with those passwords.

Probably belong to some Script-Kiddy group.
... and nationalities.

- “spargeosu#%^%&138cucapulinpicior”
• “spargeosu#%^%*&138cucapulnopicior”
• Cosmin Dumitru tipped me of: that is Romanian.
• His translation: ”sparge osul” - break the bone. ”cu capul in picior” - with head struck by foot - or something like that.
Conclusion:

People use good passwords:

Script-Kiddies use good passwords:

A reasonable amount of hosts could be penetrated with this method:
✓

Method works:
✓

All data has been anonymized and published at http://sshcb.wybt.net/:
✓
Conclusion:

People use good passwords:

- Script-Kiddies use good passwords: ✓
- A reasonable amount of hosts could be penetrated with this method: ✓
- Method works: ✓
- All data has been anonymized and published at http://sshcb.wybt.net/: ✓
Conclusion:

People use good passwords: X
Conclusion:

People use good passwords: ✗

Script-Kiddies use good passwords:
Conclusion:

People use good passwords:✗

Script-Kiddies use good passwords:✗
Conclusion:

People use good passwords: X
Script-Kiddies use good passwords: X
A reasonable amount of hosts could be penetrated with this method:
Conclusion:

People use good passwords: X
Script-Kiddies use good passwords: X
A reasonable amount of hosts could be penetrated with this method: ✓

All data has been anonymized and published at http://sshcb.wybt.net/
Conclusion:

People use good passwords: ×
Script-Kiddies use good passwords: ×
A reasonable amount of hosts could be penetrated with this method: ✓
Method works:
Conclusion:

People use good passwords: ✗
Script-Kiddies use good passwords: ✗
A reasonable amount of hosts could be penetrated with this method: ✓
Method works: ✓
Conclusion:

- People use good passwords: ✗
- Script-Kiddies use good passwords: ✗
- A reasonable amount of hosts could be penetrated with this method: ✓
- Method works: ✓
- All data has been anonymized and published at http://sshcb.wybt.net:/
Conclusion:

People use good passwords: X
Script-Kiddies use good passwords: X
A reasonable amount of hosts could be penetrated with this method: ✓
Method works: ✓
All data has been anonymized and published at http://sshcb.wybt.net/: ✓
Last remarks:

Thanks to all the people providing support, resources and even sponsoring!

**Pieter Lexis** - Told me to stop talking and test the theory.
**Dr. Hans Dijkman** - Gave huge support in solving the ethical and legal issues of this work.
**Nadine Donaldson, BSc** - Gave helpful advise on the data analysis.
**Kay Rechthien** - Assisted in setting up resources and networks.
**Stefan Wahl** - Supported the project by providing LIR services for the RIPE networks.
**Niels Sijm, MSc** - Assisted in setting up resources and networks.
**Theodor Reppe** - Provided systems for the single host study.

Greetings to **Elmo Todurov** from the University of Tallinn, who independently had the same idea during the finalisation of this research.