Defining and Evaluating Greynets (Sparse Darknets)

Warren Harrop,
Grenville Armitage
{wazz,garmitage}@swin.edu.au

Outline

• Darknet Background
• Previous work
• Enterprise and campus darknets
• Terminology
  • Defining and characterising a greynet
  • Terms and definitions
• Analysis
  • Establishing the efficacy of a greynet
• Conclusion
Darknet Background

- A darknet can be a component of an Intrusion Detection System (IDS)
- Monitors unused IP address space
- Key assumption: packets heading for darknet IP addresses - should not be
- We can use this information to infer ongoing and potential network issues

Previous Work

- Emphasis on inferring wider Internet activity
  - “Size” of darknet is important here
    - Internet Motion Sensor (IMS)
    - Network telescope (caida)
    - Cymru darknet project
  - Spinning cube of potential doom – worthy of note
    - Unique visualisation of darknet data
Enterprise and Campus Darknets

• Intent is different to a “traditional” darknet

• An “internal” darknet
  • Important for inferring local rather than wide area activity

• Scan activity within the enterprise network is of great concern
  • The source is already inside outer defenses
  • Automate detection and clamp-down the source?

Defining and Characterising a Greynet

• Greynets are collections of non-contiguous blocks of IP addresses
  • “Dark” in the traditional sense
  • Also interspersed among groups of “lit” (used) IP addresses

• Interspersing with valid hosts makes it harder for malware to avoid hitting greynet addresses while searching for infection targets
Greynet Terminology

Terms and Definitions

- Greynet
- Potentials
  - Set of 'dark' IP addresses that can be monitored and are unused
- Listeners
  - Set of 'dark' IP addresses being monitored (n)
- Distribution of listeners
  - Pattern of IP address distribution (X)
- Orientation of listeners
  - 'Rotation' of listeners (Θ)
Terms and Definitions

- **Greynet**
- **Potentials**
  - Set of 'dark' IP addresses that can be monitored and are unused
- **Listeners**
  - Set of 'dark' IP addresses being monitored (n)
- **Distribution of listeners**
  - Pattern of IP address distribution (X)
- **Orientation of listeners**
  - 'Rotation' of listeners (θ)

Described by the polar coordinate \((L_nX, \theta)\)

Types

- A, B

A greynet with an even distribution of potential and listener hosts within it with offset \(\theta\)
Implementation and Analysis

Establishing the Efficacy of a Greynet

- Two metrics defined for analysis
  - Time to detect (TTD) and median inter-event interval
- Data gathered experimentally from a live darknet
  - 238 contiguous 'dark' IP addresses open to the Internet
  - Simulation run on full data set to simulate various configuration of greynet
Experimental setup

136.186.x.N
Where N is 16 to 254

136.186.x.0/24

136.186.0.0/16

Campus LAN

Internet

Experimental Results
Summary of packets observed by the full greynet
(Trace time ≈ 3.5 months)

Port 445 Malware (96.8%) Due to firewall 1 RSVP path

<table>
<thead>
<tr>
<th></th>
<th>TCP</th>
<th>UDP</th>
<th>ICMP</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>993,431</td>
<td>0</td>
<td>717</td>
<td>994,148</td>
</tr>
<tr>
<td>External</td>
<td>1,734,286</td>
<td>315,243</td>
<td>121,750</td>
<td>2,171,280</td>
</tr>
<tr>
<td>Total</td>
<td>2,727,717</td>
<td>315,243</td>
<td>122,467</td>
<td>3,165,428</td>
</tr>
</tbody>
</table>

99% “Winpopups” of these:
62% Fraudulent Windows update
24% Male genitalia enlargement processes
1.3% “non accredited degrees”
Experimental Results

“Host 174's” TCP scans on port 445 analysed using a series of “type A” greynets increasing in listener numbers (n)

LCN-05
http://caia.swin.edu.au (wazz,garmitage)@swin.edu.au November, 2005 Page 18
Experimental Results

Externally sourced TCP events analysed using a series of “type B” greynets increasing in listeners (n) and rotated by θ

- To detect sasser infected hosts in < 200 sec
  - 30 greynet hosts
- TCP scans that move linearly across address space
  - With only one listener
  - Less than 2.5 sec to detect
Conclusion

- Greynet – 'dark' IP addresses dispersed among 'lit' IP addresses
- Proposed description of greynets - \((L^n, \theta)\)
- Initial experiments - synthesise various greynets from small 238 address darknet over 3 months
- Ideas:
  - Greynet address assignment should be integrated with DHCP
  - A single host on a VLAN trunk switch port could instantiate greynets simultaneously on multiple subnets