

CENTRE FOR ADVANCED INTERNET ARCHITECTURES

#### Greynets: A Definition and Evaluation of Sparsely Populated Darknets

Warren Harrop, Grenville Armitage

{wazz,garmitage}@swin.edu.au

### **Outline**

- Background
- Previous work
- Enterprise and campus darknets
- Defining and characterising a greynet
- Terms and definitions
- 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 doing so
- Infer ongoing and potential network issues



MineNet-05

http://caia.swin.edu.au {wazz,garmitage}@swin.edu.au August 26th, 2005 Page 3

# **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
  - 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 your outer defenses
  - Automate detection and clamp-down of source?



# **Defining and Characterising a Greynet**

- A Greynet is a collection of non-contiguous blocks of "dark" IP addresses
  - "Dark" unused and unadvertised

MineNet-05

- Interspersed among groups of "lit" (in-use) IP addresses
- Interspersing with valid hosts makes it harder for malware to avoid hitting greynet addresses while searching for infection targets



http://caia.swin.edu.au {wazz,garmitage}@swin.edu.au August 26th, 2005 Page 5

# **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)



A greynet with an even distribution of potential and listener hosts within it with offset  $\theta$ 



## Described by the coordinate $(L_n X, \theta)$

http://caia.swin.edu.au {wazz,garmitage}@swin.edu.au August 26th, 2005 Page 7

# **Establishing the Efficacy of a Greynet**

• Two metrics defined for analysis

MineNet-05

- 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 configurations of greynet





#### **Experimental Results**

- 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
    - Extended version of this work will appear at IEEE Conference on Local Computer Networks (LCN), Sydney November 2005



```
MineNet-05
```

#### http://caia.swin.edu.au {wazz,garmitage}@swin.edu.au August 26th, 2005 Page 9

## Conclusion

- Greynet 'dark' IP addresses dispersed among 'lit' IP addresses
- Proposed description of greynets  $(L_nX, \theta)$
- 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

