Teaching Flow Analysis with Live Flow Data

Alex Musicante, City of Pittsburgh
John Dwyer, Student, Carnegie Mellon University
Sid Faber, Adjunct Faculty, Carnegie Mellon University
...or
Pittsburgh’s Three Rivers of Flow

Alex Musicante, City of Pittsburgh
John Dwyer, Student, Carnegie Mellon University
Sid Faber, Adjunct Faculty, Carnegie Mellon University
About the City

• Org Structure
  – Politicians
  – IT

• Network Structure
Partnership

• History of projects between CMU and the City
  – Heinz College
  – Information Systems & Management
  – Public Policy and Management

• “Penetration Test” project last year
  – Technical exercise
  – Policy assessment and recommendations
Adding Flow

• Initiated discussions with the CIO
• Review & approval by City Legal, CMU Legal, others
• Volunteers installed a sensor at the primary internet connection
The Class

• Network Situational Awareness class
  – Instructors:
    • Tim Shimeall*
    • Sid Faber
  – Anonymized data
    • MAWI, Internet 2, CDX
The Project

• Gain Network Situational Awareness
• Provide information back to the city
• Done in the blind
The Process

- Find Heavy Hitters
- Create a profile
- Eliminate bogons
- Monitor over time
Discussions

- ACL / Least Privilege
- DNS
- Policy Validation
  - Remote Access (Gotomypc)
  - Streaming Video
Results

• Network Profile
  – Scans
  – Client Web, Served Web
  – Servers as Clients
  – Email
  – DNS
  – NTP
  – Etc.
Shameful Advertisement: Prism
Traffic Volume by Port/Service (bytes)

- **bytes**
- **packets**
- **flows**

**Total**
- IN: 3.19 MB/s, 1:00
- OUT: 0.4 MB/s, 19:00

**Scans**
- IN: 1.31 MB/s, 10:00
- OUT: 5.46 MB/s, 17:00

**Client Web**
- IN: 1.33 MB/s, 10:00
- OUT: 5.10 MB/s, 19:00

**Served Web**
- IN: 371 KB/s, 20:00
- OUT: 13.3 KB/s, 21:00

**Servers as Clients**
- IN: 0.18 MB/s, 10:00
- OUT: 17.9 MB/s, 17:00

**Email**
- IN: 115 KB/s, 12:00
- OUT: 319 KB/s, 13:00

**DNS**
- IN: 1.74 KB/s, 16:00
Instructor Comments

• Network Situational Awareness:
  – Perceive: Network flow sensor
  – Comprehend: Network profile, leftovers
  – Project: What does this mean to me?
Instructor Comments (2)

• All packets are innocent until proven guilty
  – Profile by country
  – Scan traffic, inbound traffic
City Comments

• Leveraging university, Limited resources
• External validation
  – Support for external auditors
Student Comments

- Initial impression: too much data
- Dividing traffic led to identifying patterns
- Couldn’t really be done with full packet data
Future

- Improve the sensor
  - Instrument the cold spare
  - Instrument internally
  - Add metadata
- Add a security focus
- Add a geopolitical focus
Thank You

Alex Musicante, City of Pittsburgh
John Dwyer, Student, Carnegie Mellon University
Sid Faber, Adjunct Faculty, Carnegie Mellon University