Behavior Based Approach to Network Traffic Analysis

Rob Nelson
Casey O’Leary
Pacific Northwest National Laboratory
Issues/Challenges

• Data volume (noisy/highly dimensional)
• Watch-lists
• Data interpretation – significance
• Monitoring threats
Data Collation, Processing, Analysis, and Reporting Process
Advancing the Art

• Situation awareness
  – Recognize nefarious activities before reported
  – Focusing analysts on particular IP’s or organizations

• Novel analysis
  – Identifying exploits before well known
Dynamic Watch-lists

• External hosts
  – Those IP addresses that pose a threat against the enterprise networks

• Vulnerable hosts
  – Those internal IP address that are targets
Methods

- Weighted values associated with behavior
- Tracking over time
- Dynamic list placement
- Behavior profiles
- Multiple sources of input
External Hosts

• Actions
  – Reconnaissance
  – Exploits
• Intent
  – Collection
  – Compromise
  – Recruitment
• Methods
  – Stealth
  – Collaboration
Vulnerable Hosts

- Interacting with external hosts
- Sending unsolicited messages
- High level of chatter
- New services running
Factors

- Intent
- Temporal/frequency
- Sophistication
- Cooperation
- Enclave
Adaptability

- Dynamic weighting factors
- Methods
- Techniques
- Code
Future Efforts

- Architecture to work on raw data
  - Near real-time situation awareness
  - Parallelism of queries
- Sophisticated detection methods
- Communities
Questions

• Contacts

Rob Nelson  
rob.nelson@pnl.gov

Casey O’Leary  
casey@pnl.gov