LOGS AND OTHER IMPORTANT SYSTEMS FILES

49th Security Division - Education Night

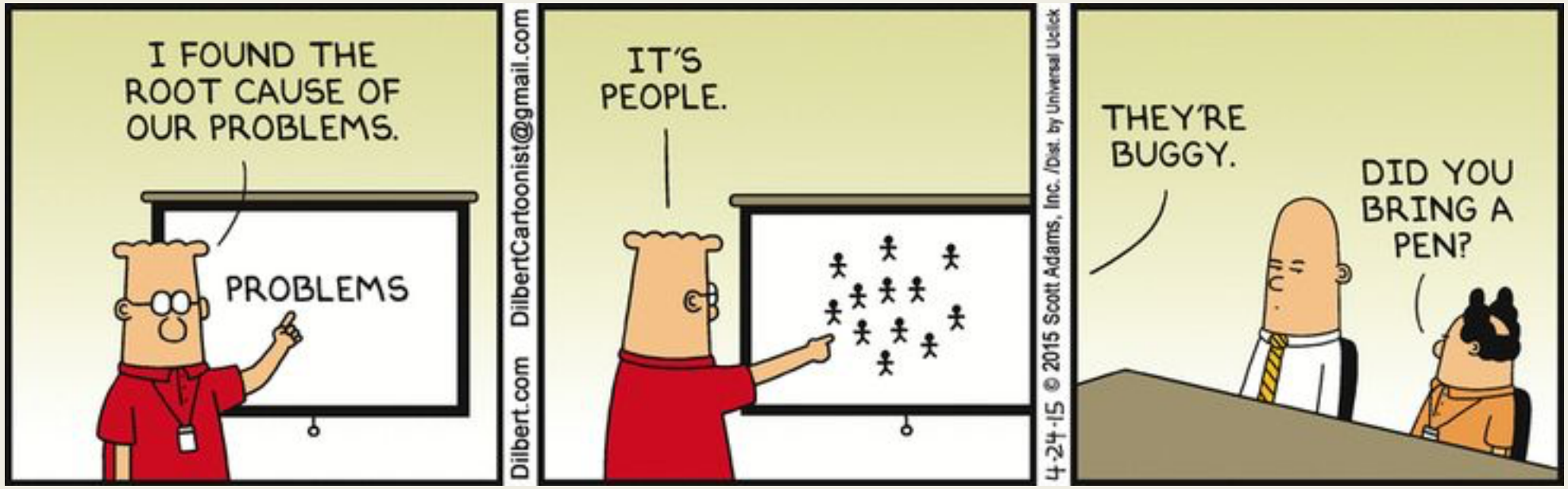
Announcements

- Remote Competition Practices
  - https://vr0n.tech/ctf/ for the file
  - http://vr0n.tech:8000 for the CTF
- Google meet will be provided in slack
  - *PlaidCTF April 17th – April 19th*
  - *NCL Team Game April 17th – April 19th*

Logs

- What are Logs?
- Who looks at logs?
- Why are they important?

Root Cause Analysis



Root Cause Analysis

- Questions to ask
  - *What Changed?*
  - *What is Broken?*
  - *When did it broken (When is it broken)?*
  - *Etc.*
- Example (what would you do):
  - *A service isn't responding to specific requests, what do you do?*
- Real life example (Linux forums)

NCL (aws_vpc_flow.log)

- Demo
- How would you solve?
  - *Find the IP with the 5th highest packet transfer recorded?*
    - Bash Solution

      sed 1d aws_vpc_flow.log | awk '{a[$4] += $9} END{for (i in a) print i, a[i]}' | sort -r -n -k 2 | head -n 5

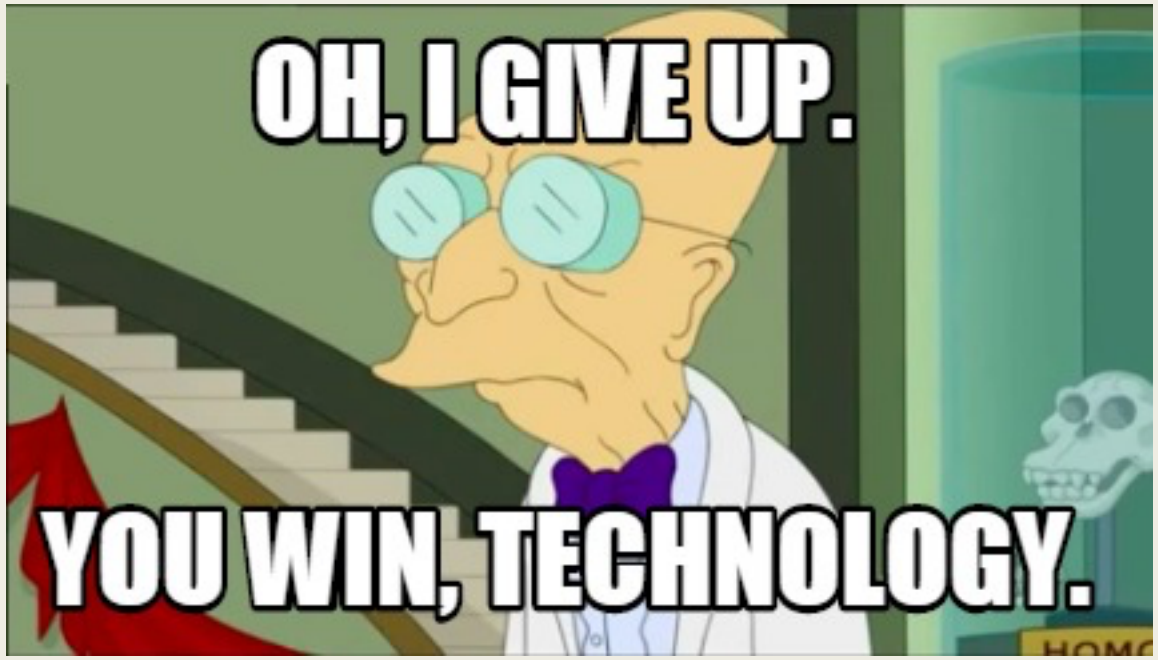
    - Python Solution

System Specific

- Unix
  - *Log files*
    - /var/log
    - Unix System Logging
  - *Configuration Files*
    - /etc
- Windows
  - Event Viewer
  - Windows Cheat Sheet for Important Files
- Mac OS

Tooling

- Visualization Tools
  - *Grafana (Open Source)*
  - *LogDNA*
- *Indexing and Search*
  - *Apache Lucene (Open Source)*
- CLI Tools
  - *GoAccess (Open Source)*
  - *Lnav (Open Source)*
- Roll it yourself…
  - *Python (csv, json, etc.)*
  - *Bash*
    - Awk (Open Source)



Management Tools, etc.

- Analyzing Logs at Scale
- SIEM
  - *Splunk*
    - (Free) vs (30 Day Enterprise Trial)
  - *ELK Stack (Elasticsearch, Logstash, Kibana) (Open Source)*
    - Graylog (Open Source)
  - *Alien Vault*

Interesting Projects

- Loglizer
  - *machine learning-based log analysis toolkit for automated anomaly detection*
- Dsiem
  - *Security event correlation engine for ELK Stack*
- … Root Cause Analysis (Paper)

Resources

- Github Awesome Log Analysis
- Ultimate Guide to Logging
- Trail of Bits CTF Reference
- Parsing Log Files with Python example
  - *Github Example*
  - *Blog Post*
- Linux Log Files
- Getting Started with Kibana (ELK Stack)
- PacketLife (CheatSheet)