DISA
Defense Information Systems Agency
Department of Defense

Lessons Learned while providing SiLK Training

Jim Downey, DISA

Disclaimer

The views are the authors alone and do not necessarily reflect the Defense Information Systems Agency. This is for information purposes only. No warranty of any kind is expressed or implied.

About me

- Worked in a CSIRT as: Incident Analysis and Coordination, Penetration Testing, Antivirus support. Worked with SiLK on and off since 2002.

- Most of what I’m saying is first hand, but we’ve had other trainers too.

Some variables and some constants

- Topics stayed largely the same over this discussion. Trained analysts on SiLK along with a few other tools (visualization, scan database, iSiLK) built using SiLK
- Started with real data and context, migrated towards obfuscated data
- Used different facilities and gear at different times
- Only recently started pre-testing for Unix proficiency
- No pre-testing for TCP/IP familiarity

Facilities

- **Our customers are in roughly six different time zones**

- **Our own facility:**
  - **Having a CAC doesn’t mean having a certificate on that CAC.**
  - **Live training via teleconferencing difficult to do and almost impossible to do effectively with in person students at the same time**

- **Customer provided facilities:**
  - **Insist on testing full connection including usernames and passwords (at least one!) before you jump on that plane. Then quietly check against your data server’s logs.**
  - **Just because it works on one workstation doesn’t mean all the workstations on a network have the same browser configuration.**
  - **Just because a commercial version of SSH client is installed doesn’t mean the customer’s firewall allows tcp/22 outbound to the training server.**
  - **If you’ve never seen pictures or been before, and the customer says there’s an overhead projector, bring a pointer in case it’s beyond arms reach.**

The tools

- SiLK installed easily on Linux environment. iSiLK installed easily under Windows without System Admin privileges (your mileage may vary).

- At least one Unix (Ubuntu) environment where iSiLK client doesn’t work. Open source software doesn’t necessarily mean it’ll work on an Open Source Operating System.

- rwrandomize could potentially be replaced with a process vice a simple tool, as others have suggested

Training Data

- If you can train on real data, with context, that’s the most compelling to a student.
- If you obfuscate your data, save the map! We later added asset data and had to grab new netflow data to have them similarly obfuscated.
- Keep the general types of use cases, even if you change the names, locations, dates, etc. Otherwise, looses interest.
- For obfuscated data, we used a couple of /16s plus added some additional flow data covering a Denial of Service attack, and changed the IPs and times.

Students & Training Material

- A fair number of students had forgotten some important details about TCP like the 3 way handshake.
- A fair number had minimal experience with Unix, a few were software developers.
- Highlights found in SEI (or other existing or easily created material) are sufficient for the above cases.

I’ve been trained, now what?

- Users may not know what to do with flow data other than scope and impact based on IDS alerts.
  - Know the users overall mission and business processes
    - Integrate with this where it makes sense
    - Advocate rescoping where it makes sense
    - You may have to do a lot of the reworking
- Users may not have the skills to build out processes.
  - You may find it useful to write scripts, provide mappings, etc yourself.
  - Someone has to maintain these