# Brainstorm Information

Sandia
National
Laboratories

Materials

- **Butcher Paper**
  - **Provides a large area to work with**
  - **Portable and storable (temporarily)**

- **Post-Its**
  - **Used to record ideas**
  - **<u>All</u> ideas should be written down**

- **Sharpie Markers**
 - **Easy to read at a distance so all participants can see current ideas**

Brainstorming

Sandia National Laboratories
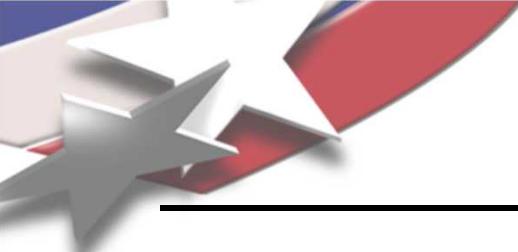
What is this?
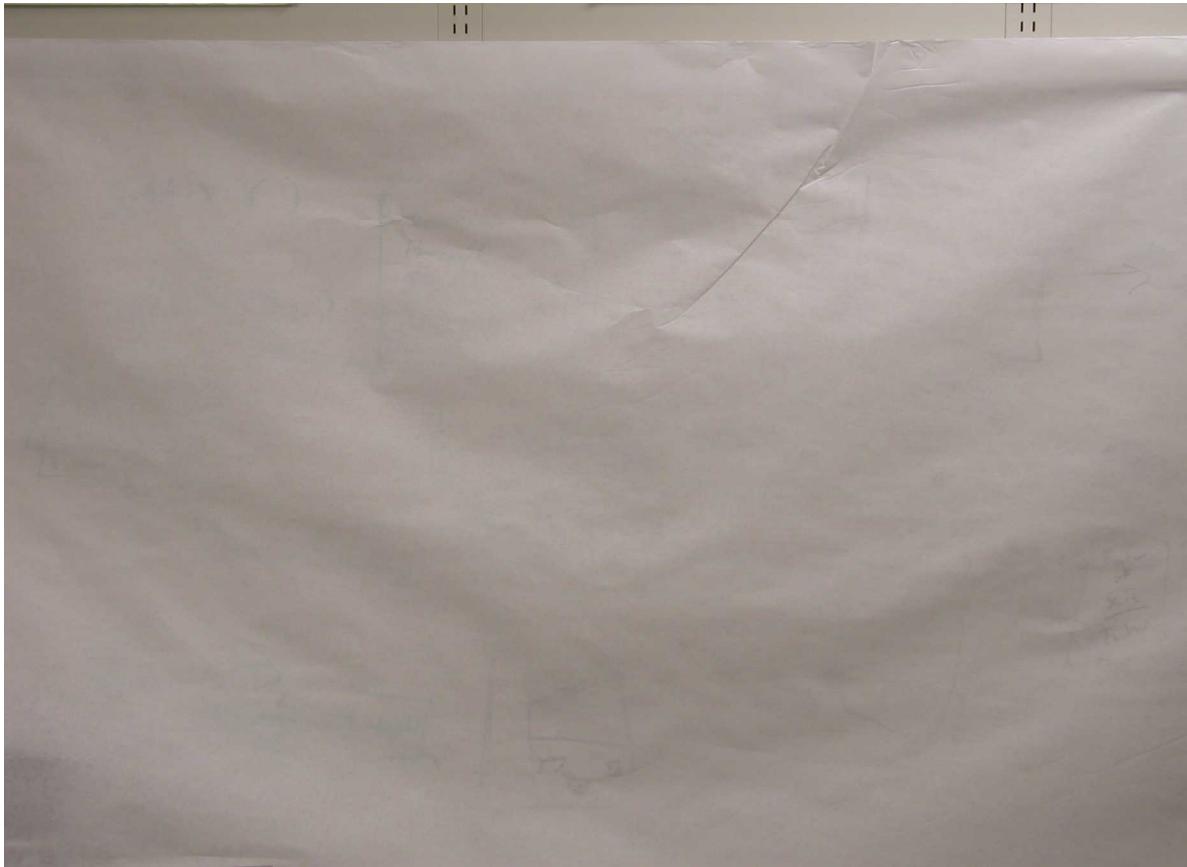
# Butcher Paper!

- **This is what we have given you to start with... A completely blank slate!**

- **Now what?**

Sandia National Laboratories

Start Points and Flags

Sandia National Laboratories

Attack!!

RT3.0-6
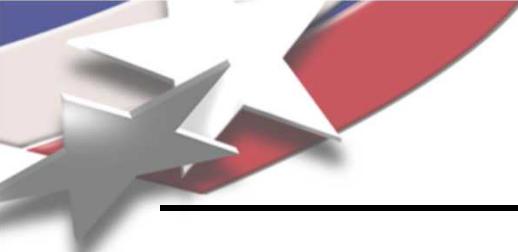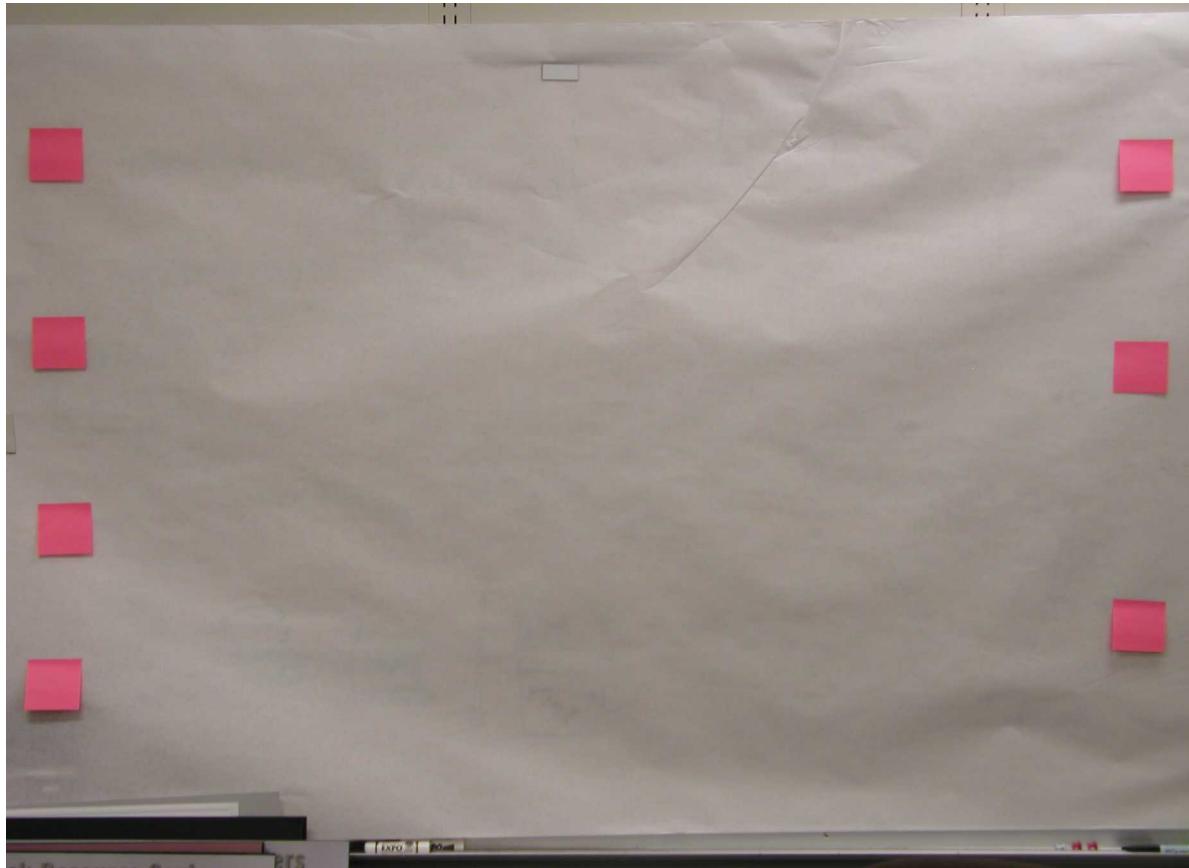
Organization

- **Once the team starts winding down and wrapping up ideas, start to organize the attacks**

- **This is often done in a group so ideas can be clarified (post-its are small!)**

- **When you think you have the order, start drawing lines**
  - **We recommend using light color markers for the first cut**

Sandia National Laboratories

Attack Graph

Sandia National Laboratories
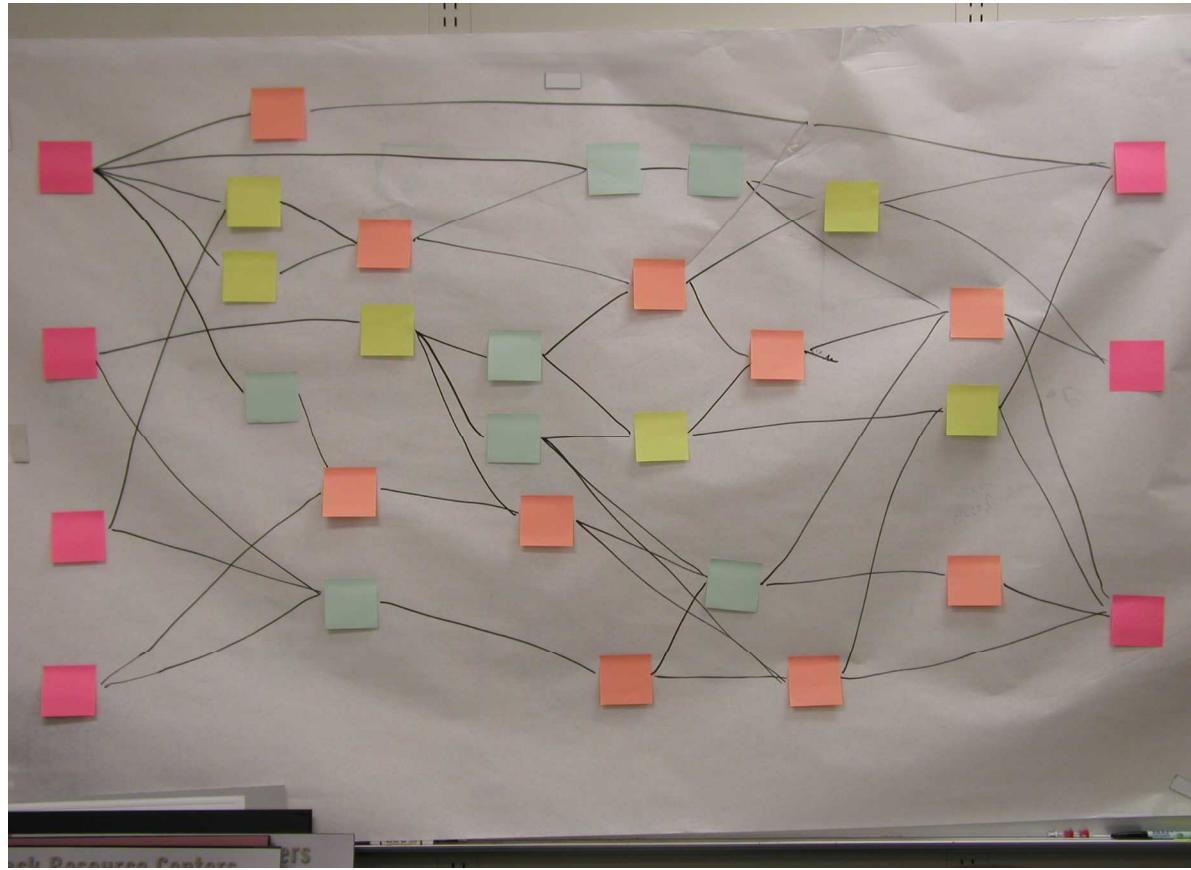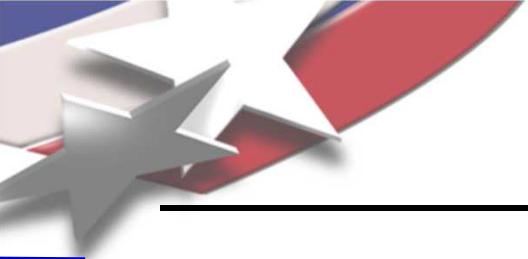
Attack Graphs

- **Once you are comfortable with the graph and lines, re-trace the lines in a dark color so they are visible**

- **If you are going to be moving the butcher paper, reinforce the post-its with tape**
  - **There's nothing worse than losing post-its unless its having them, but not knowing where they go!**

Sandia National Laboratories
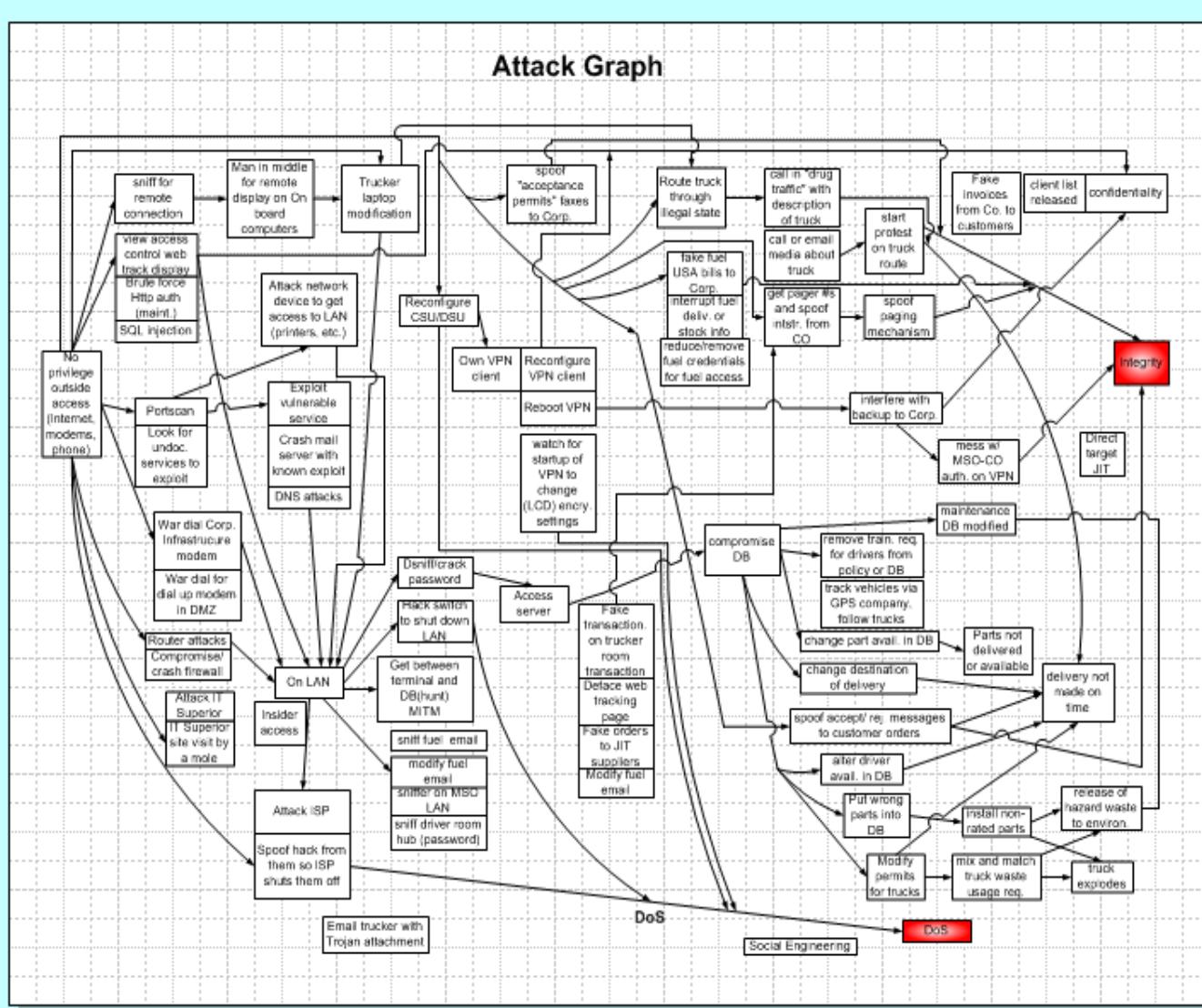
Attack Graph

Reality Check

- **After the attack graph has been developed, the core members of the red team must review the suggested attacks to ensure that attacks are reasonable and achievable**

Brainstorming

Sandia National Laboratories
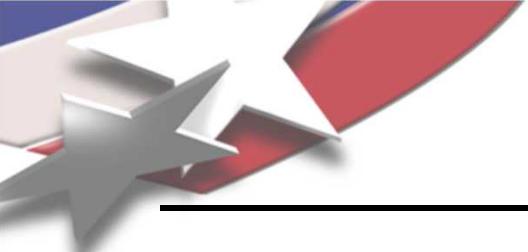
Adversary Filtering

- **Once the unrealistic attacks have been removed, the team considers the attack graph with the skills, resources, constraints of the adversary being modeled.**

- **Attacks that are beyond the capabilities of the desired adversary will be removed.**
  - **These attacks should be archived for possible later use**

Brainstorming

Sandia National Laboratories

More Constraints

- **Next, we screen out attacks based on exercise constraints/rules of engagement or other exercise requirements.**

- **In a paper exercise, this may not be necessary.**

RT3.0-13

Brainstorming

Sandia National Laboratories
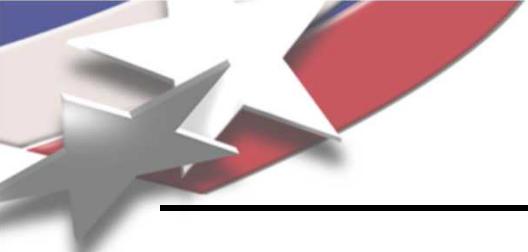
Path Grading

- **The filtered attack graph is then reviewed again to find the "best" attack path.**

- **The definition of best varies depending on the desired characteristics:**
  - **Stealth,**
  - **Cost**
  - **Time**
  - **Etc.**

Brainstorming

Sandia National Laboratories

Attack Planning - Brainstorming

RT3.0-15