# Offensive Security

Quentin Young
LUG @ NC STATE

# Topics

- Profiling & info gathering
- Analysis & research
- Vulnerability types
- Ethics

# Profiling & Information Gathering

- Before you can attack a system, you need to know:
  - What is your *objective*?
  - What *vectors* are available?
  - What *defenses* are in place?
  - Which *people* are of concern?
- Not always possible to know all of these
- More information→higher chances of success

# Profiling & Information Gathering

- Relevant information sometimes depends on objective
  - Denial of service?
  - Defacement?
  - Information retrieval?
  - Remote root?
  - Physical access?

# Profiling & Information Gathering

- Network mapping & scanning
  - nmap
- Use technical means to discover
  - What hosts exist
  - What services they are running
    - Versions
  - Who configured them and for what purpose

# Profiling & Information Gathering

- Social engineering
  - Human element is the weakest link in security
  - Often easiest to simply ask for information
  - Example:
    - John Brennan
  - Pretexting
- Necessary to build a map of the relevant people involved with the target system(s)

# Profiling & Information Gathering

-