



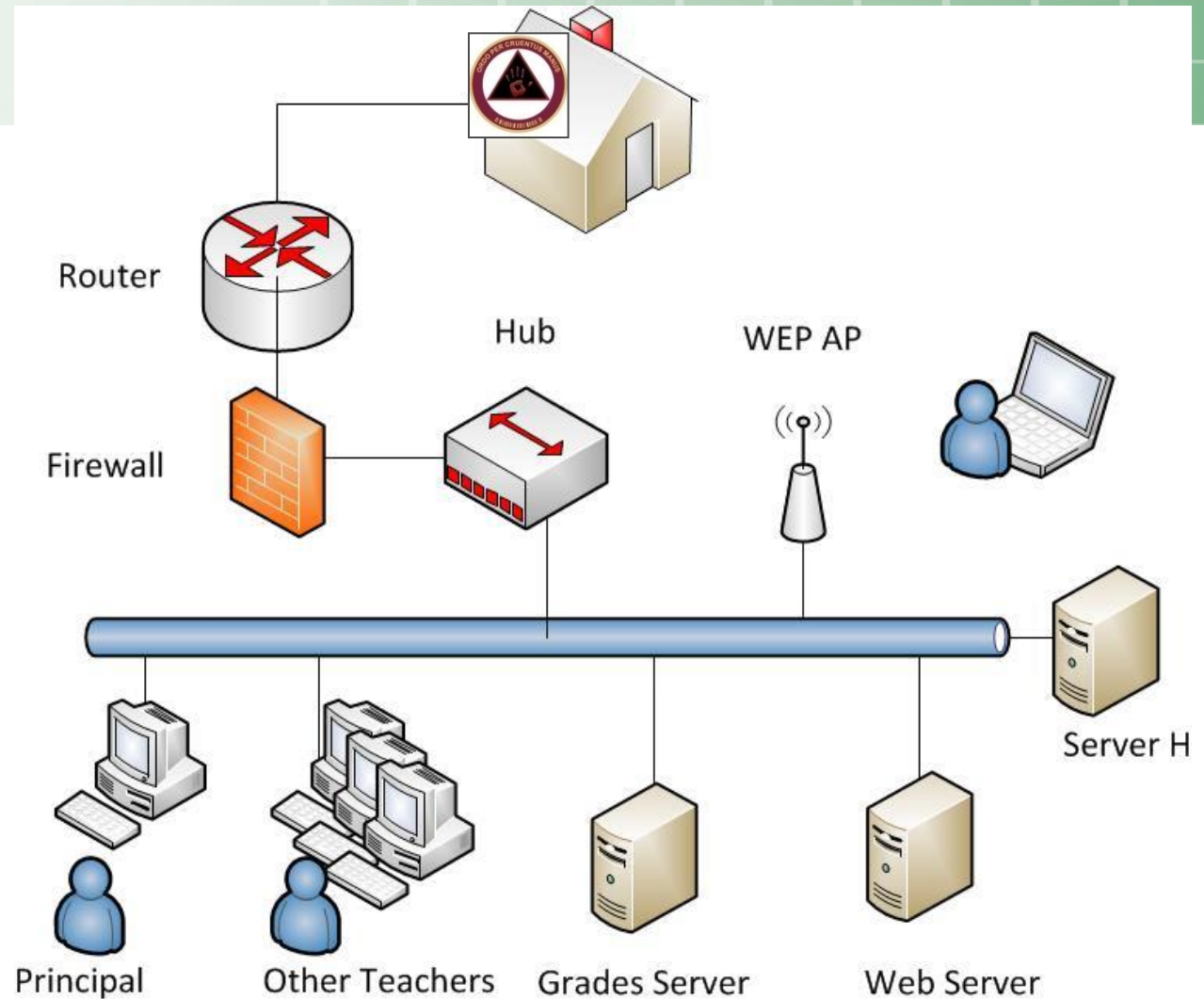
**LT James Dietle (USN)
Red Team Division Officer, Navy Information
Operations Command
Norfolk, VA**



PENTEST METHODOLOGY

The 5 minute pen test!

1. Document Review
2. Scan
3. Gain Access
4. Exploit
5. Document Findings





CHALLENGES

- Systems have a long life cycle
 - Systems are designed for years and last for years
 - Numerous systems
- It is difficult to measure a successful test
 - What does 50 Category 1 vulnerabilities mean?
 - How do you know if a test is better?
- Compliance is a checklist and not a process
 - Do the boxes really make sense?



MOVING FORWARD

- Leadership need to adequately understand cyber risk
 - **Not too much, Not too little, Just right.**
- The earlier you test the more money you typically save
 - **Good DT&E and OT&E saves money!**
- Understand the potential threats
 - **To protect against Nation States focus on quality tests**
 - **To stop Script Kiddies quantity may suffice**