Notes Security+ 2

* External pen testers – expertise, credentials, focus, experience, outside perspective
* Internal – lack of expertise, reluctance to reveal
* Purple team – providing red team with blue team knowledge and blue team with red team knowledge
* ROE – timing, scope, (environment, internal/external targets, physical locations, virtual locations/IPs/subnets, exclusions), authorization, types of exploits to use, communication/contact info, cleanup/artifacts, reporting
* Pen test phases – recon (active/passive, OSINT), penetration
* Frameworks – NIST, ISO, AICPA, CIS, CSA