



Security Exercises and Training

THREAT MANAGEMENT

Beyond a PenTest

- Security exercises can put penetration testers and defenders against each other to provide additional training
- Performed in a simulated environment...not production network
- Conducted by three types of teams:
 Red, Blue, and White

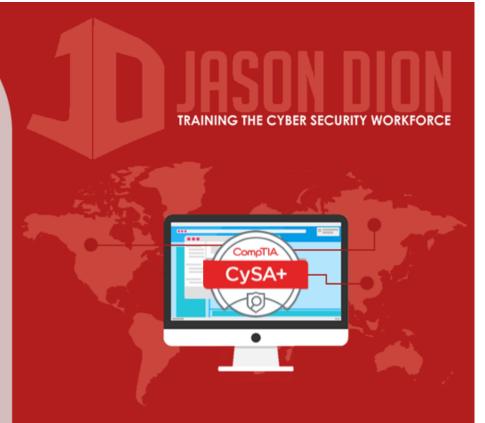


Red Team

Participates as the attacker

 Uses reconnaissance and exploitation tools to gain access to the network

Similar to penetration testers

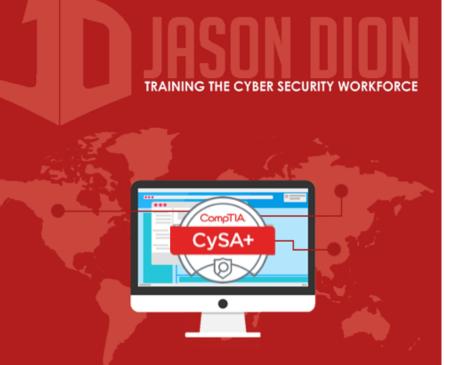


Blue Team

Participates as the defender

 Secures the network and attempts to keep red team out through the use of security controls

 Usually made up of system and network administrators



White Team

Participates as the referee

Coordinates the exercise and arbitrates disputes

 Maintains the simulated environment and monitors the exercise

