JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA
CySA+

Passive Reconnaissance

THREAT MANAGEMENT

Passive Reconnaissance

- More difficult than active reconnaissance

- Relies on logs and other data

- Data you receive may be out of date

- Often used during a cyber incident response

Log and Configuration Analysis

- Local system configuration data and log files can be used to build a network map

- Some tools exist to parse configuration files into a usable topology

- Much of this is done manually, though