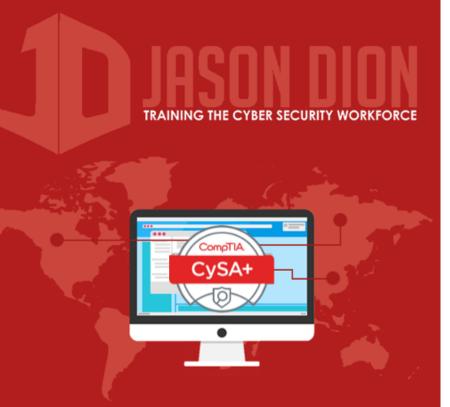# Footprinting the Network

## THREAT MANAGEMENT

# Footprinting the Network

- Creates a map of the network, systems, and other infrastructure of the company

- Created using a mixture of information gathering tools and manual research

- Guidance can be found in the NIST SP 800-115 and the Open Source Security Testing Methodology Manual (OSSTMM)

# Active Reconnaissance

- Utilizes host scanning tools to gather information about systems, services, and vulnerabilities in the network

- Does not include exploitation of the vulnerabilities, only identification of them

- Permission should be sought out before conducting active reconnaissance because it could be construed as an attack by mistake

CompTIA
CySA+