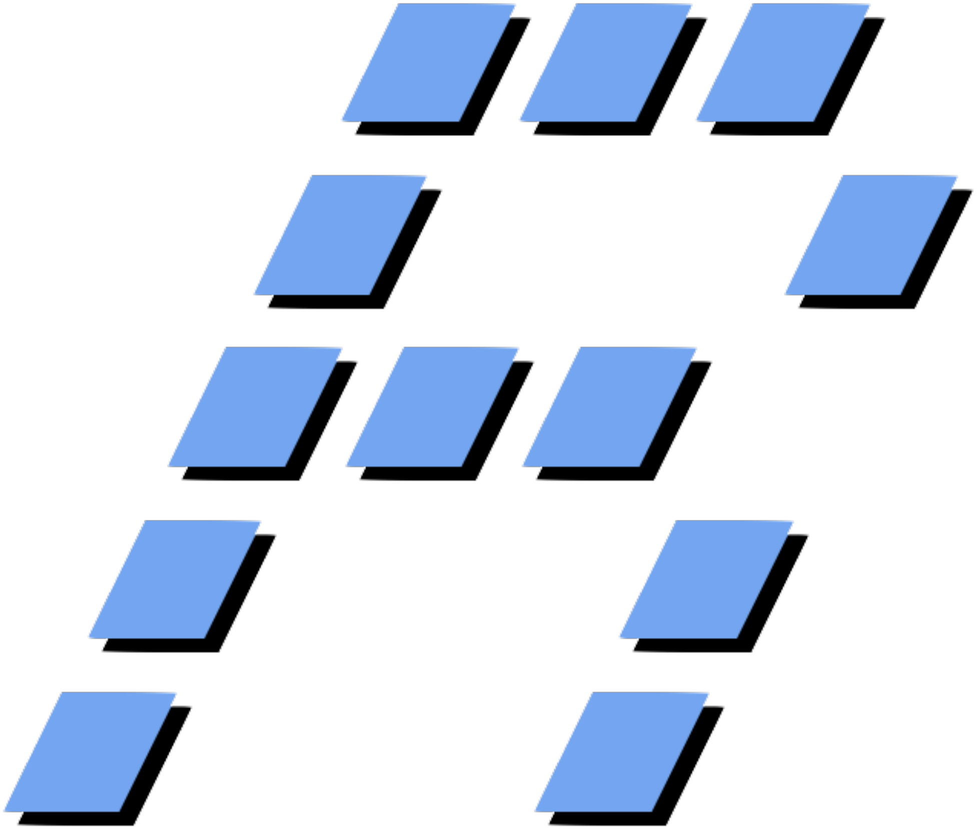
Technical Information Gathering with Recon-ng

Tim Tomes

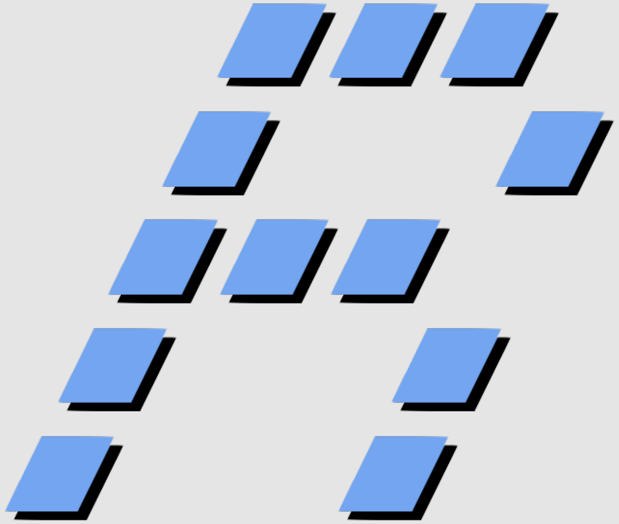
SECURITY ENGINEER – WEB APPLICATION SECURITY

@lanmaster53 www.lanmaster53.com



Creator: Tim “lanmaster53” Tomes

Feature rich reconnaissance framework designed with the goal of providing a powerful environment to quickly and thoroughly conduct open source web-based reconnaissance.

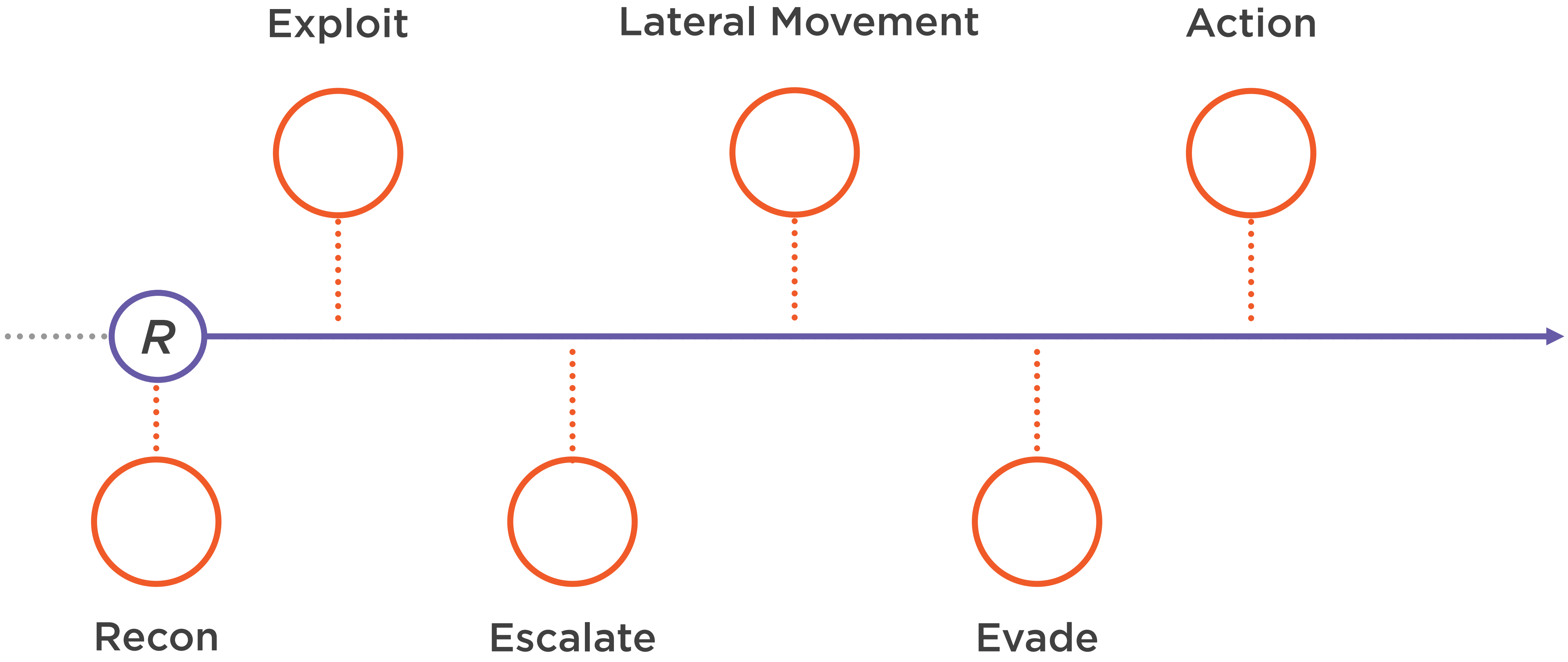


Open source framework providing a powerful environment to automate open source web-based reconnaissance

Available at recon-ng.com for download with complete documentation for usage on the wiki

Cross platform, one-stop shop that removes the need to maintain a collection of information gathering scripts

Kill Chain



Exploit

Lateral Movement

Action

Recon

Escalate

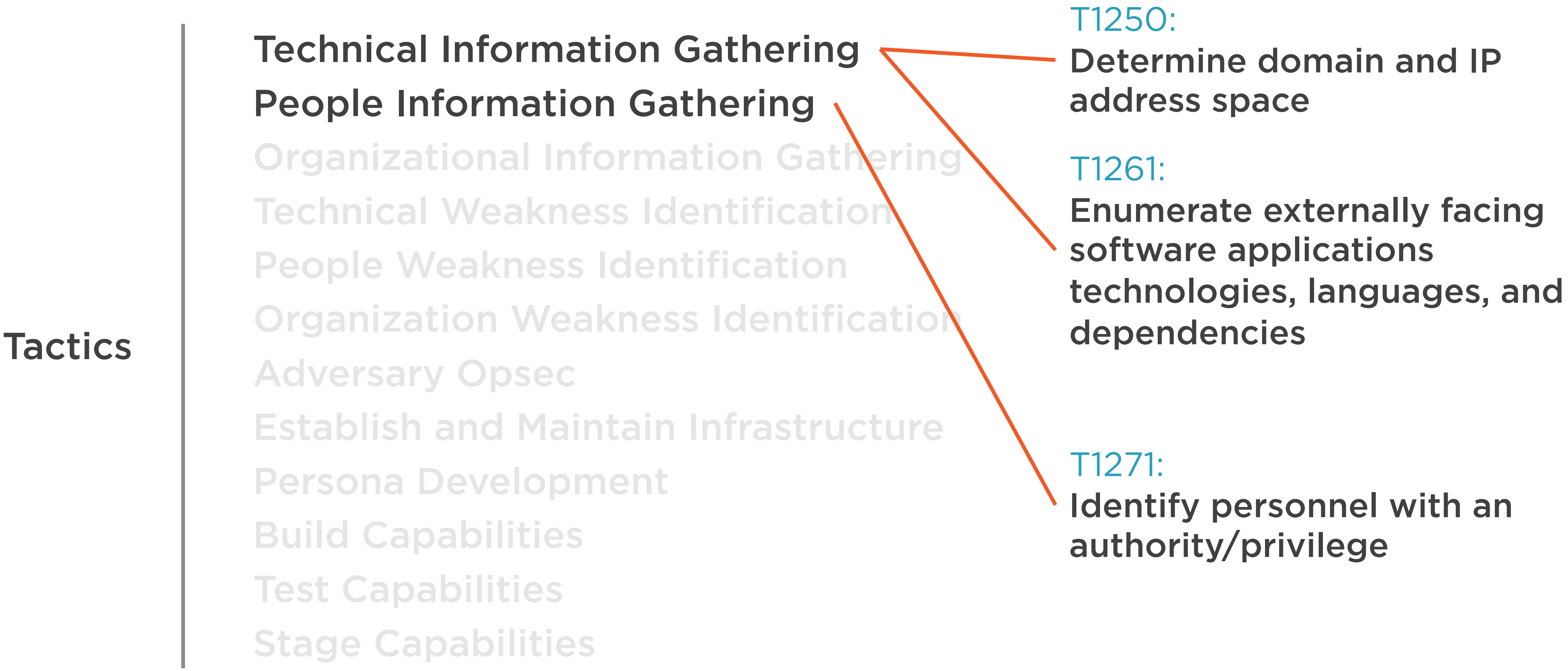
Evade

MITRE PRE-ATT&CK

Tactics

- Technical Information Gathering
- People Information Gathering
- Organizational Information Gathering
- Technical Weakness Identification
- People Weakness Identification
- Organization Weakness Identification
- Adversary Opsec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

MITRE PRE-ATT&CK



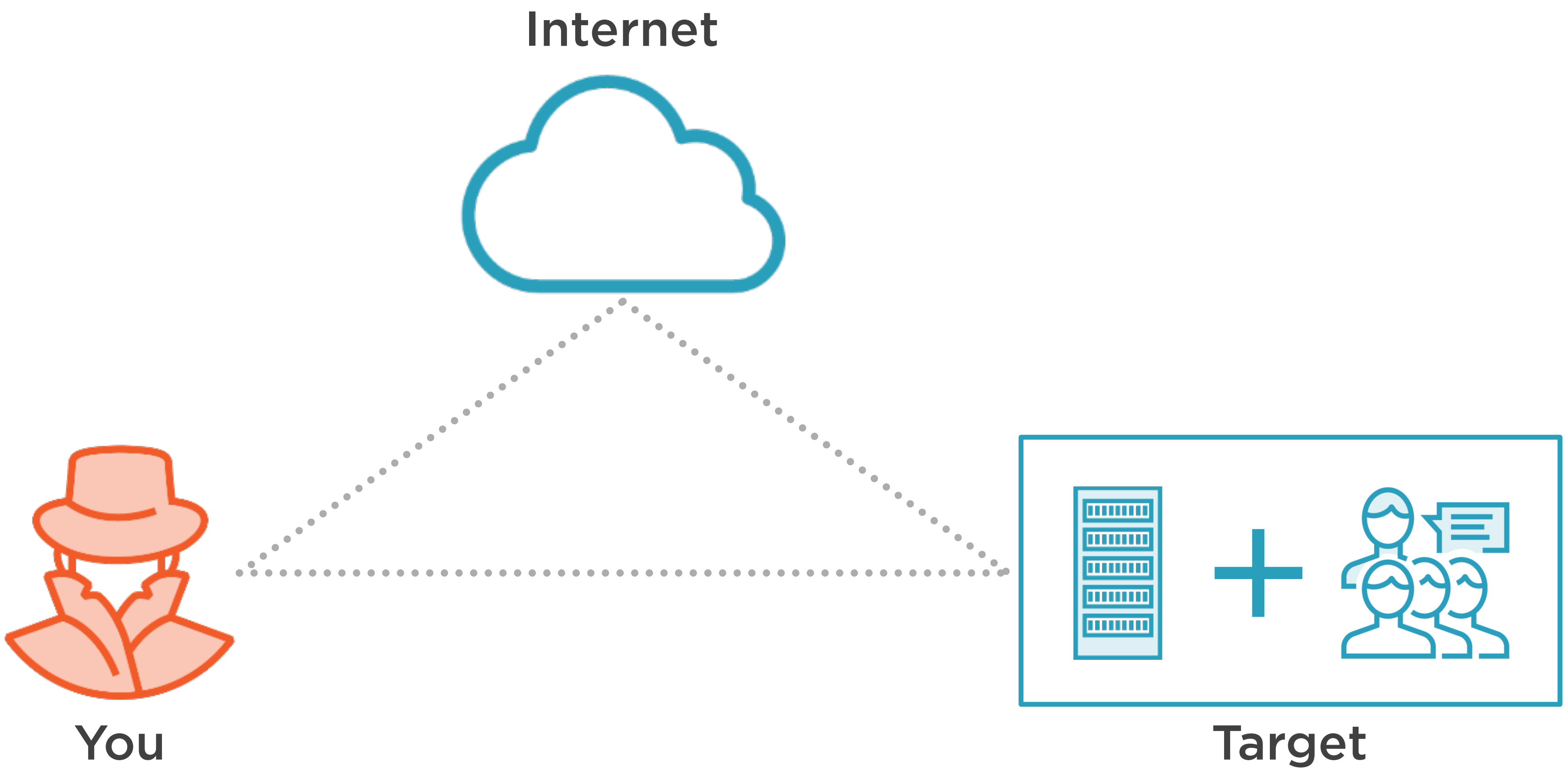
Tactics

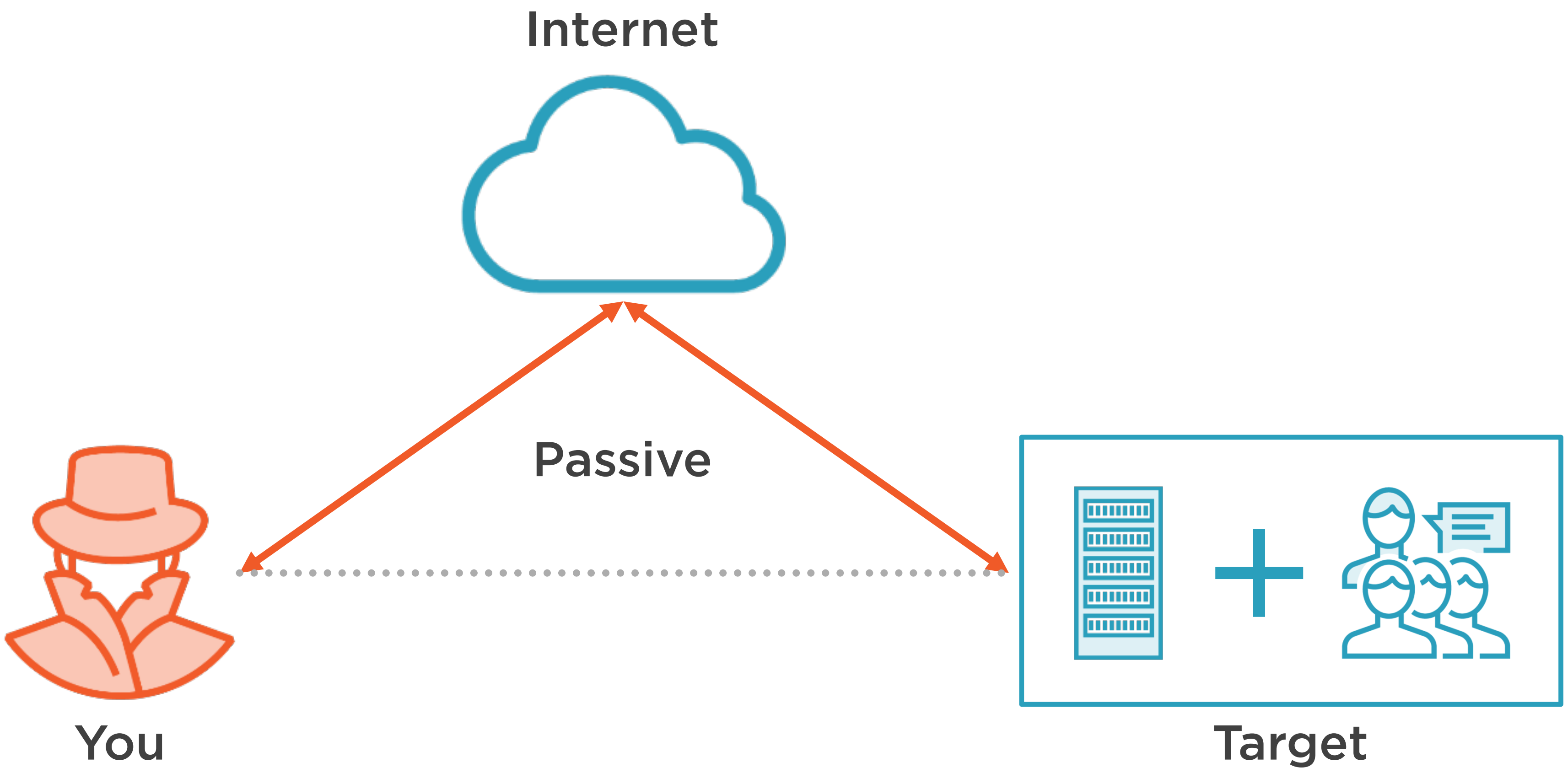
- Technical Information Gathering
- People Information Gathering
- Organizational Information Gathering
- Technical Weakness Identification
- People Weakness Identification
- Organization Weakness Identification
- Adversary Opsec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

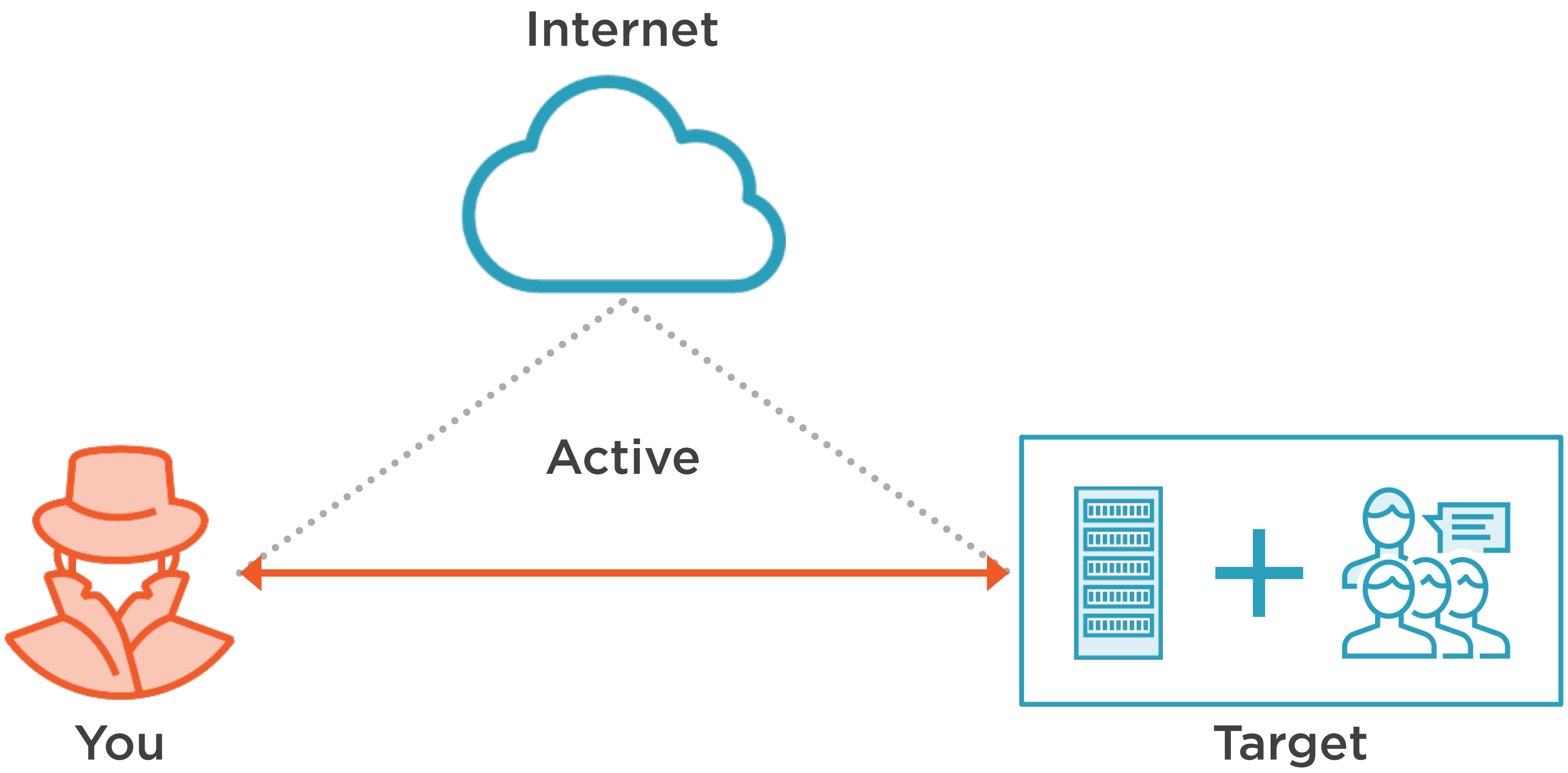
T1250:
Determine domain and IP address space

T1261:
Enumerate externally facing software applications technologies, languages, and dependencies

T1271:
Identify personnel with an authority/privilege


Internet
You
+
Target


Internet
Passive
You
Target


Internet
Active
You
Target