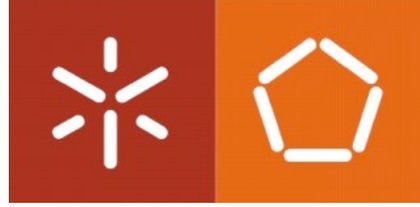
Universidade do Minho
Departamento de Informática



Tecnologia de Segurança

João Marco Silva
joaomarco@di.uminho.pt

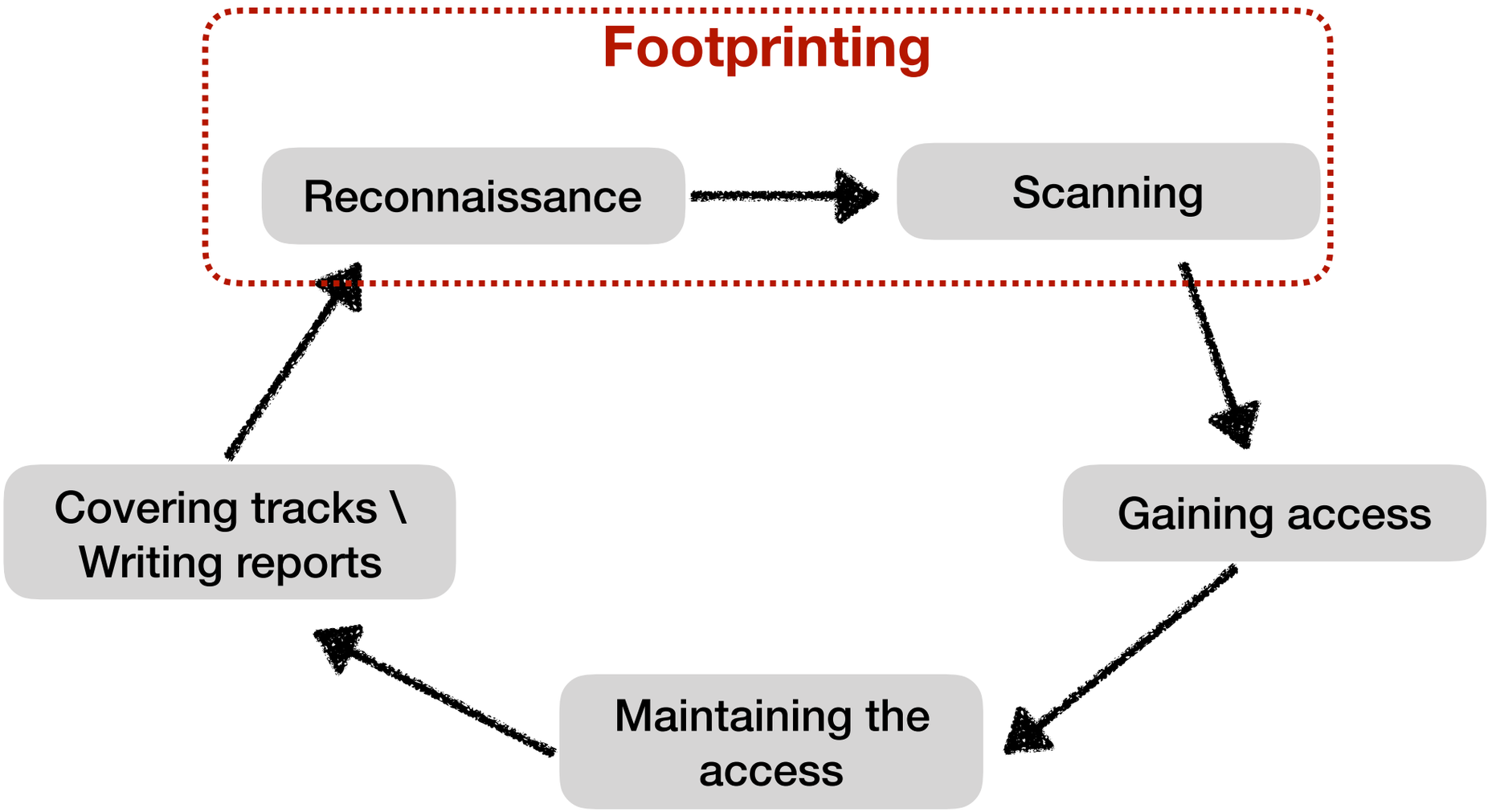
Penetration Testing

- Authorised attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems

- “Ethical hacking”

Penetration Testing

- Cyclical 5 stages process



Penetration Testing

- Footprinting
  - passive (reconnaissance) or active (scanning) information gathering about some target
  - enable an attacker to create a near complete profile of an organisation’s security posture

Penetration Testing

- Internal source
  - DNS information
  - private websites
  - dumpster diving
  - shoulder surfing
  - eavesdropping

Penetration Testing

- External source
  - Basic tools
    - phone
    - network
    - websites
    - email header

Penetration Testing

- External source
  - Services
    - Web site
    - social network
    - whois
    - DNS
    - Archive sites archive.org
    - URL analysis
    - Source code
    - Search engine
    - Job vacancy