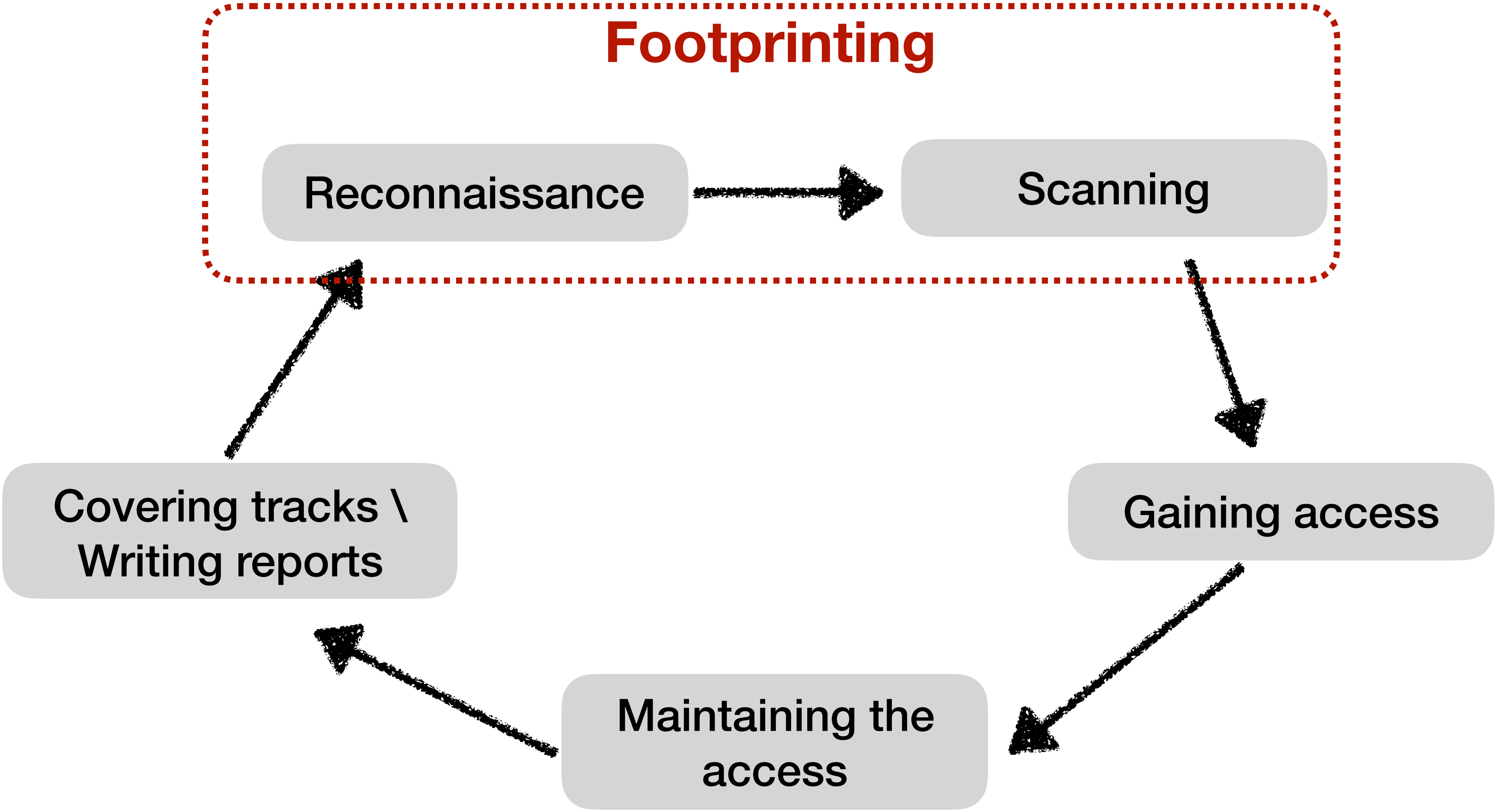
Universidade do Minho
Departamento de Informática

Tecnologia de Segurança

João Marco Silva
joaomarco@di.uminho.pt

Penetration Testing

- Cyclical 5 stages process



Penetration Testing

We will use the information acquired during the reconnaissance stage to shape probes and communicate directly with targets with the intent of identifying potential threats and vulnerabilities

- To do so, it is required to know
  - specifics about the Operating System (OS)
  - what services are available on the server
  - application version information

Penetration Testing

- Passive vs Active scanning
  - a tradeoff between detectability and depth of information
- Use public vulnerability databases to determine if the target system might be vulnerable to attack
- In this phase, there is no exploiting activities
  - it is an auditing process aiming to identify which risks might exist - not to prove their existence

Penetration Testing

- Scanning
  - check for live systems
  - check for open ports
  - scan beyond the IDS/Firewalls
  - banner grabbing
  - scan for vulnerabilities

Penetration Testing

- Tools
    - Nmap Security Scanner
        - install from https://nmap.org/
            - documentation https://nmap.org/book/man.html
    - vulnerability scanner
        - OpenVAS - http://www.openvas.org/
        - Nessus - https://www.tenable.com/downloads/nessus
    - Other tools might be used **https://sectools.org/tag/app-scanners/**

Penetration Testing

- Port Scanning
  - verifying the existence of the target system
  - obtaining a list of communication channels (ports) that accept connections
  - identify what applications are on the communication channels

Penetration Testing

- Port scanning
  - checking for live systems
    - ICMP - Internet Control Message Protocol (using ping)
    - ICMP might be disabled (use nmap with -sn flag)
      - -sn -> nmap ping scan (-sP in older versions)

Check if the domain server you choose in Parte-A is alive

Penetration Testing

- Port scanning
  - Most of the interesting applications from a PenTest perspective use TCP to communicate
    - Web servers
    - file transfer applications
    - databases
  - Tools use the TCP three-way handshake to identify open ports

```
# nmap -sS target
```

Penetration Testing

- Different types of scan are supported aiming to avoid being identified by a firewall
  - ACK scan (-sA)
  - FIN scan (-sF)
  - Null scan (-sN)
  - Xmas Tree scan (-sX)

Penetration Testing

- System identification
  - most application exploits are written for specific OS, so finding out the running OS is essential to identify possible vulnerabilities on the target

```
# nmap -O target
```

  - Passive OS fingerprinting
    - capturing TCP packets and analysing TTL information in order to identify manually the OS
  - Application banner also might provide such information

Penetration Testing

- Services identification
  - Banner
    - connecting to an unknown service on a port and checking if that port provides information about the service itself
      - with nmap, use the -sV flag
  - Packet analysis
    - analysing TCP/IP stack from captured packets and matching the data to known services