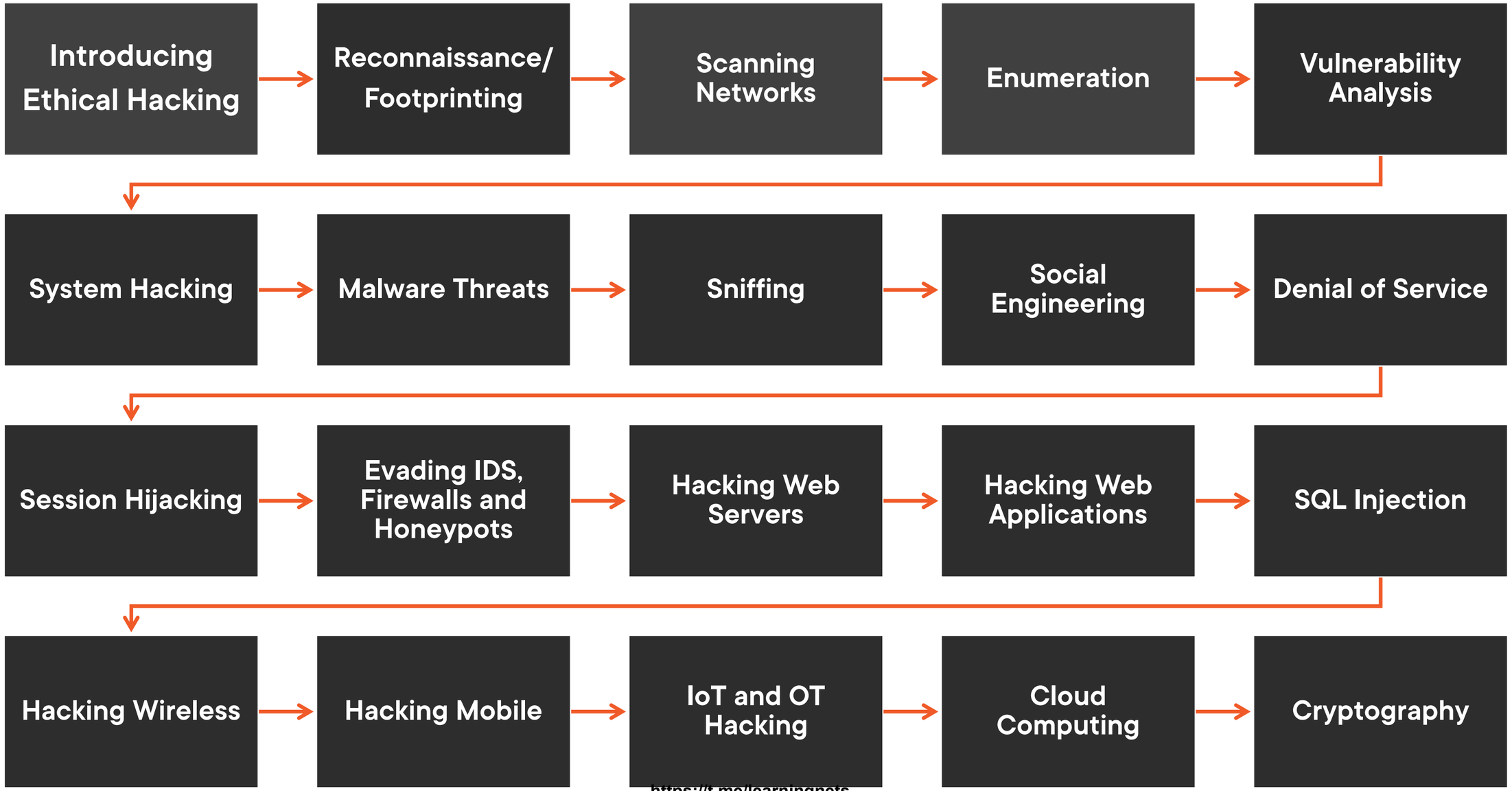
Ethical Hacking: Web Application Hacking

How to Hack Web Servers

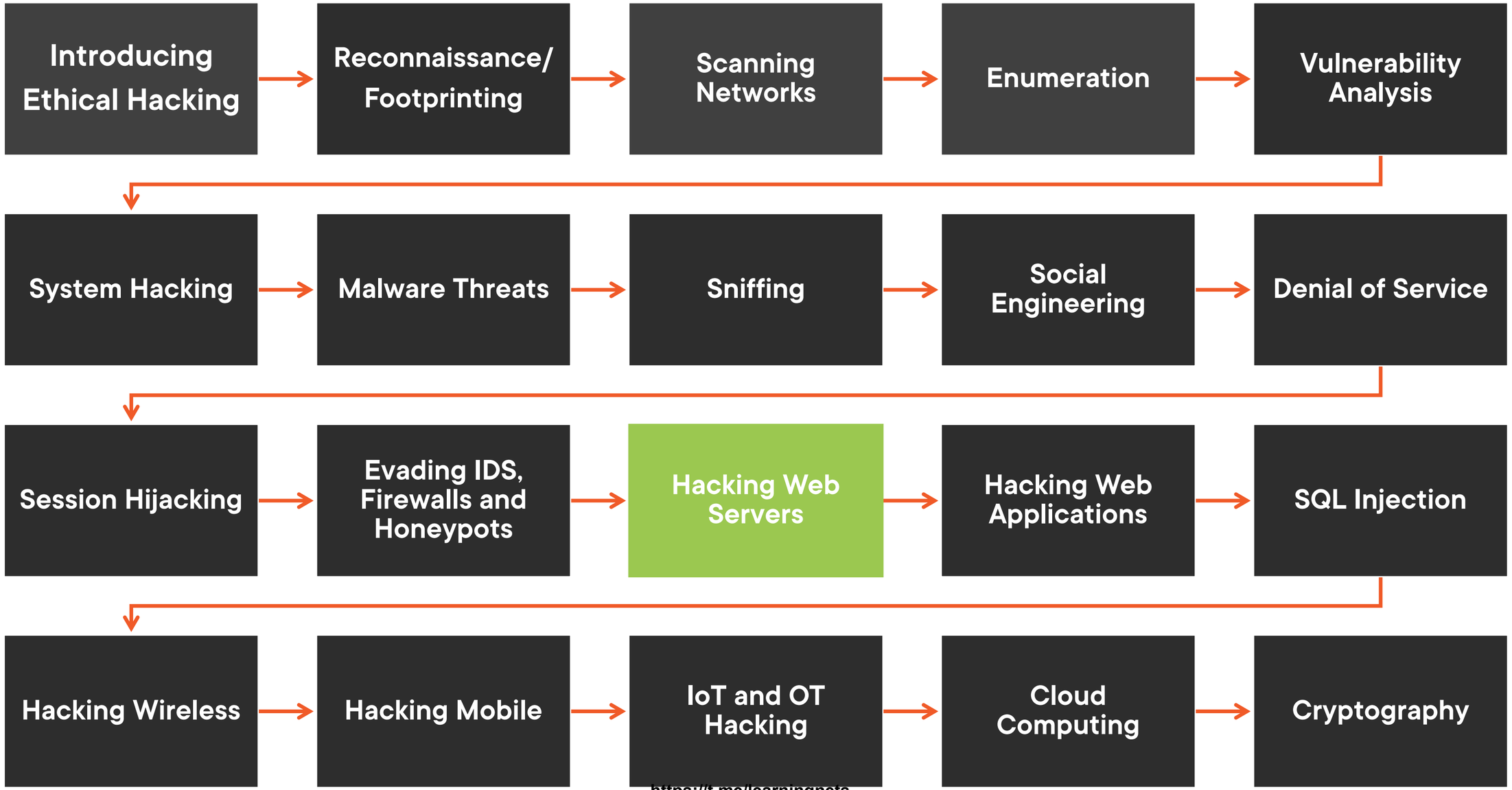
Peter Mosmans
Lead Penetration Tester

@onwebsecurity https://www.go-forward.net

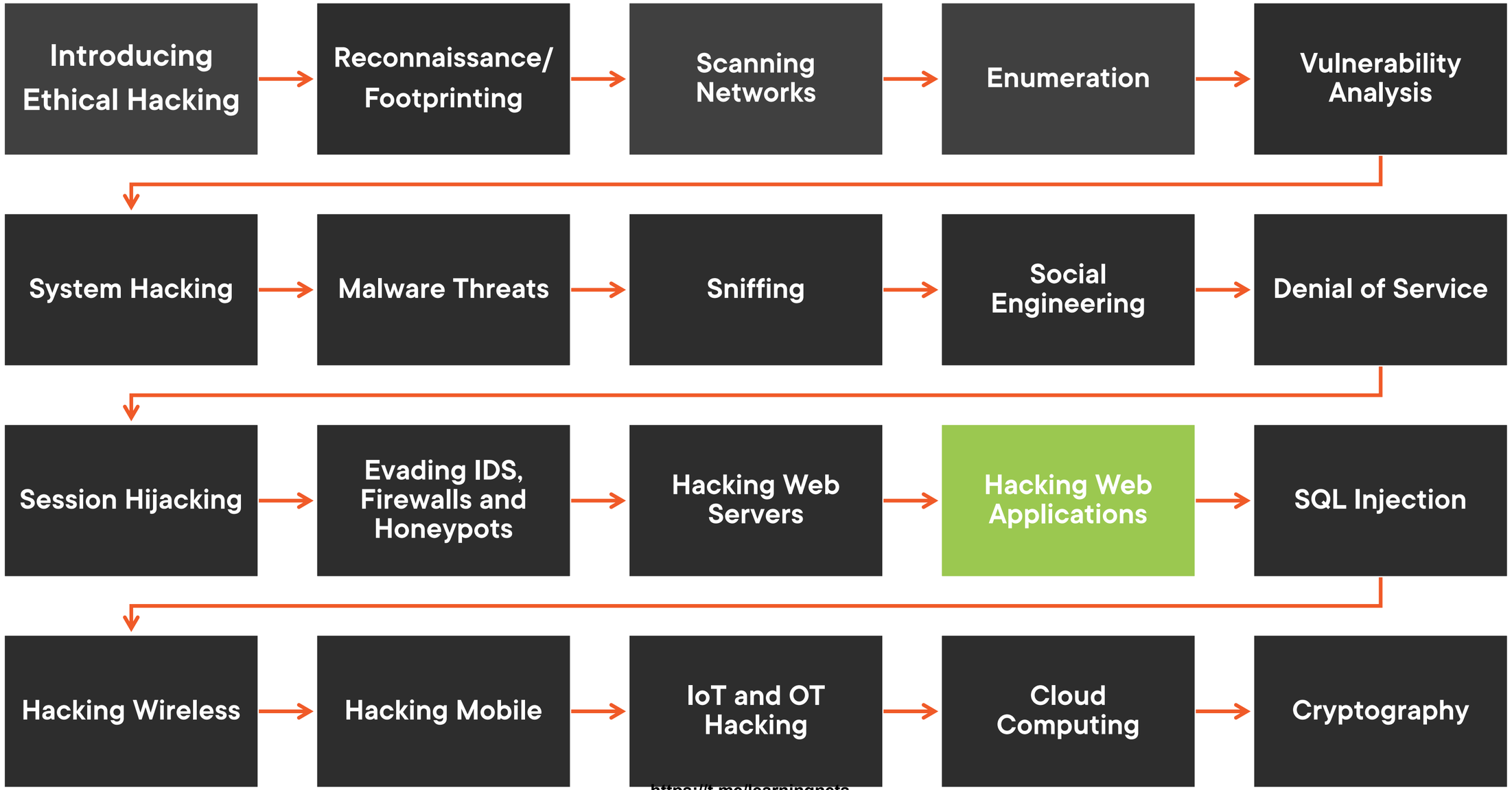
Ethical Hacking Series



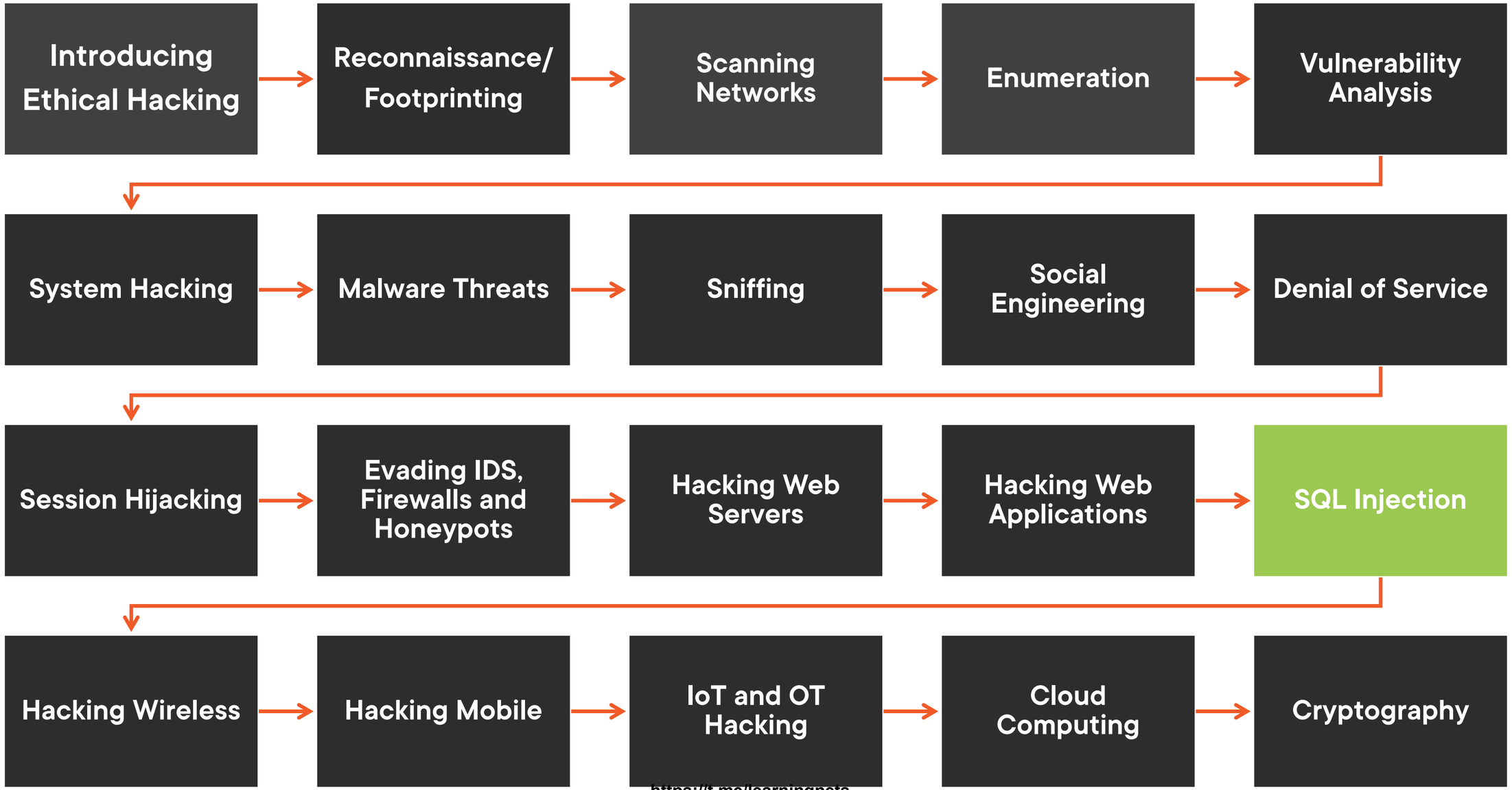
Ethical Hacking Series



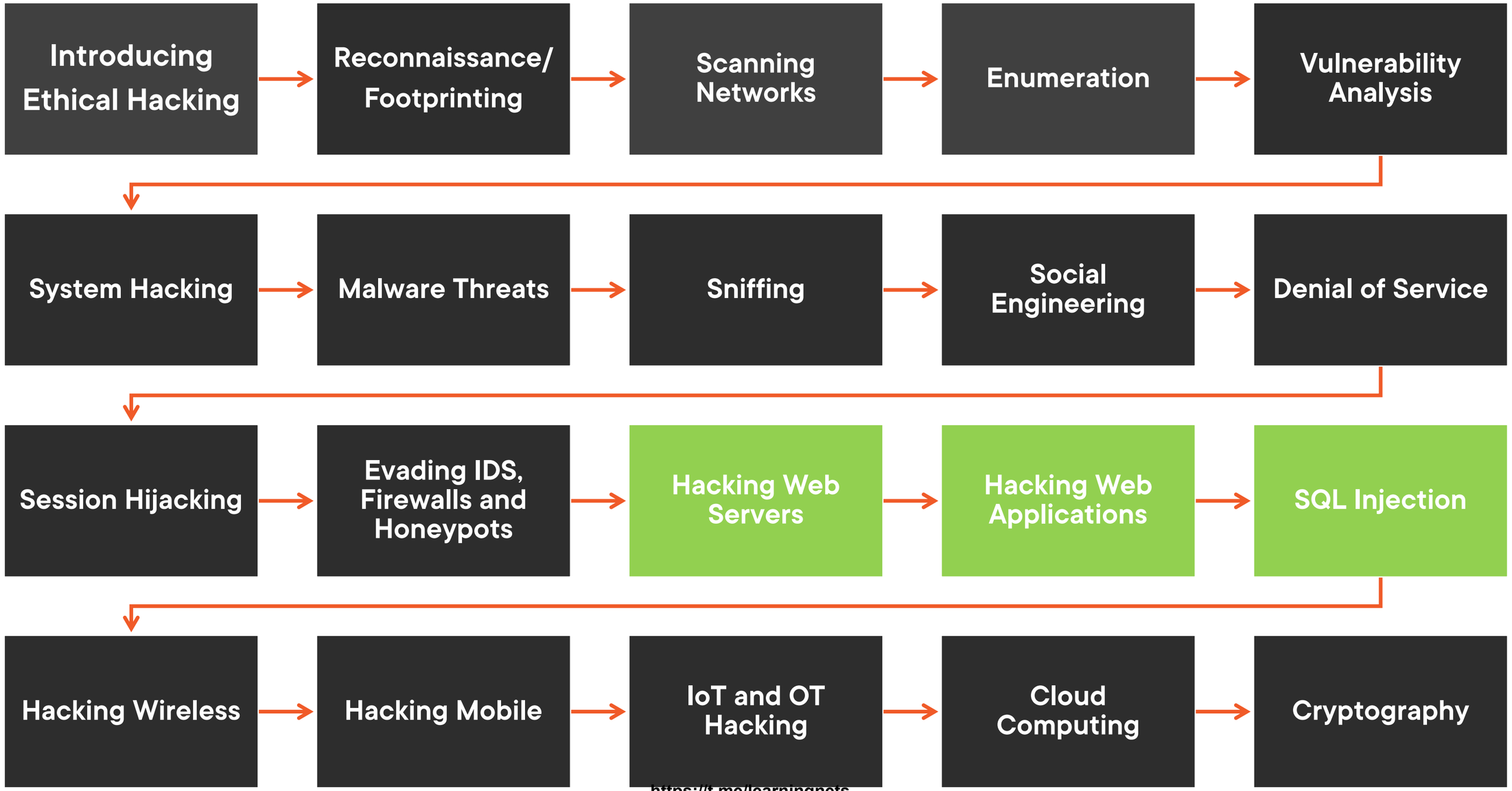
Ethical Hacking Series



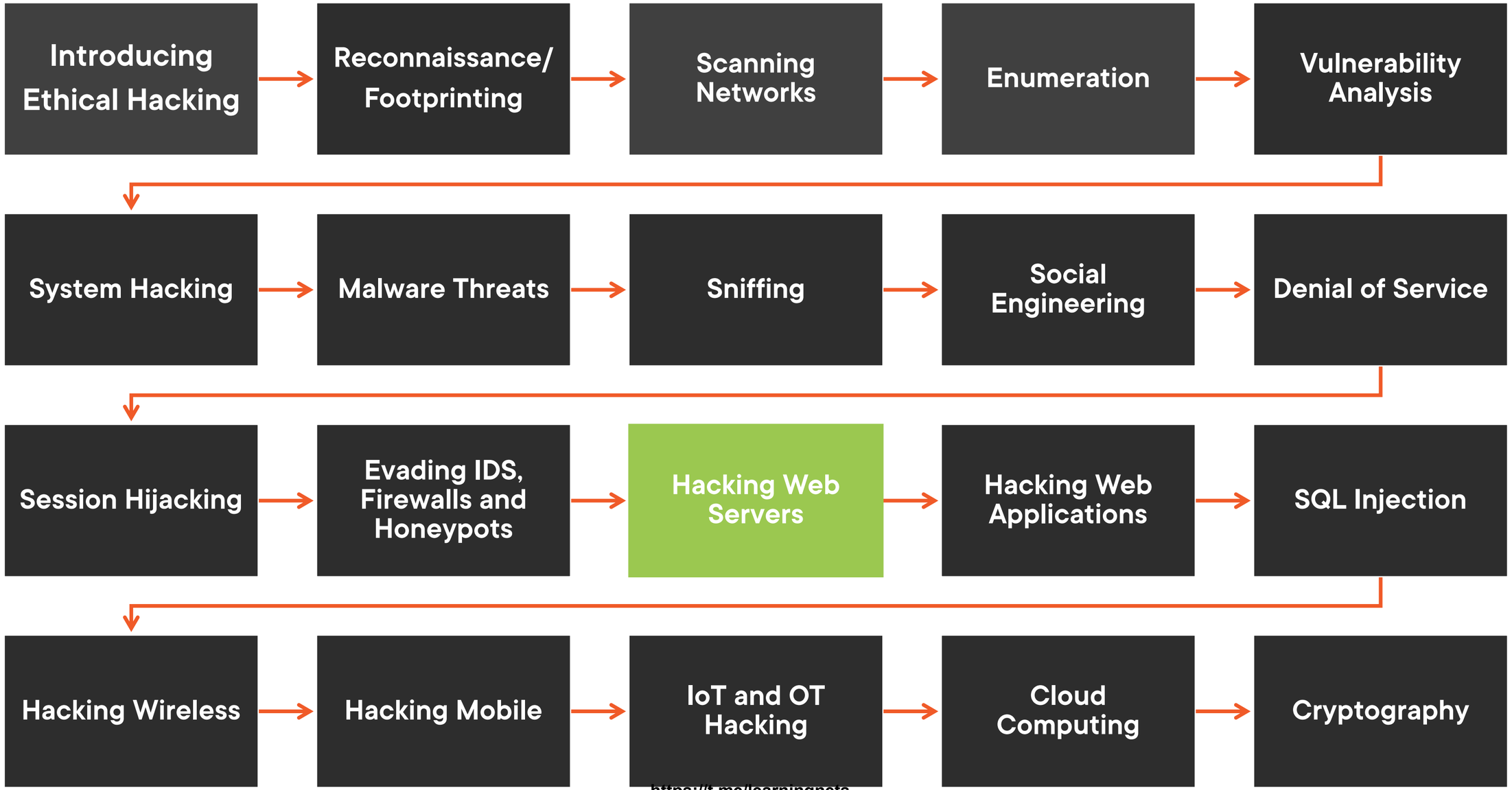
Ethical Hacking Series



Ethical Hacking Series



Ethical Hacking Series



How to Hack Web Servers

Web server concepts

Web server attacks

- **Types**
- **Methodology**
- **Tools**

Attack countermeasures

Learning check

Module review

Not many demos,
but the course materials cover
all you need to know

Web Server Concepts

Web Server

Web Server Concepts

Operating System running on the server

Web server software itself

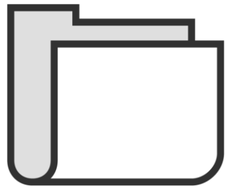
Front-end server

Serves web content

Web server maintains a connection

Terminology

Document root



Server root

Virtual hosting

Web proxy

Popular Web Server Software

HTTP Requests

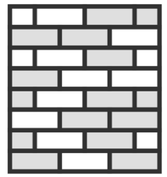
Client	Server
GET	200 OK
HEAD	2xx Success
POST	3xx Redirection
PUT	4xx Client error
DELETE	5xx Server error

Web Server Attacks

Web Server / Web Application

Attack Types

Man-in-the-Middle



Denial of service

Brute force

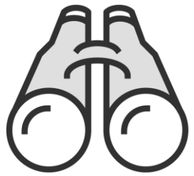
Web defacement

Web cache poisoning

Attack Methodology

- Web server information gathering
- Web server footprinting
- Website mirroring
- Vulnerability scanning
- Session hijacking
- Web server password cracking

General Penetration Testing Methodology



Reconnaissance

Finding vulnerabilities

Exploiting vulnerabilities

Post exploitation

Reporting

Web Server Attack Tools

Nikto

Nmap

Metasploit

Demo

Attacking Web Servers

- Starting Juice-Shop in the background
- Footprinting: Nmap
- Vulnerability scanning: Nikto

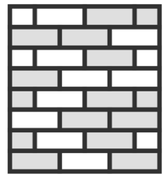
Prerequisites

- Docker installed

Web Server Attack Countermeasures

Attack Types

Man-in-the-Middle



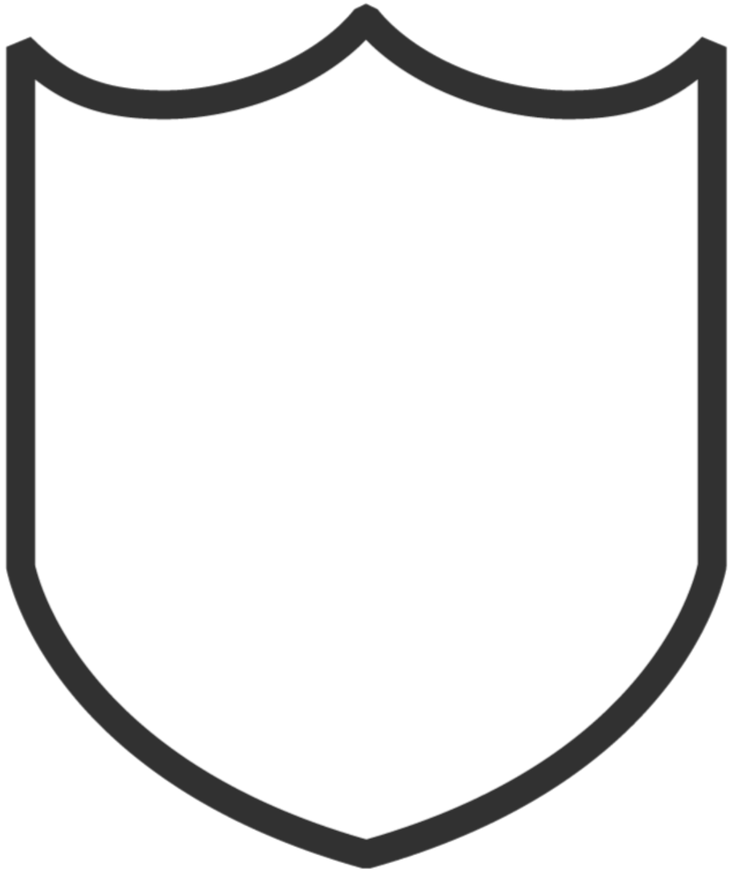
Denial of service

Brute force

Web defacement

Web cache poisoning

Web Server Countermeasures



- Encryption / certificates
- Hardening
- Rate limiting
- Patch management
- Network firewall
- Network segmentation

Learning Check

Learning Check

- Proxy server
- Vulnerability scanning
- Brute force attack
- Hardening
- Network firewall

Module Review

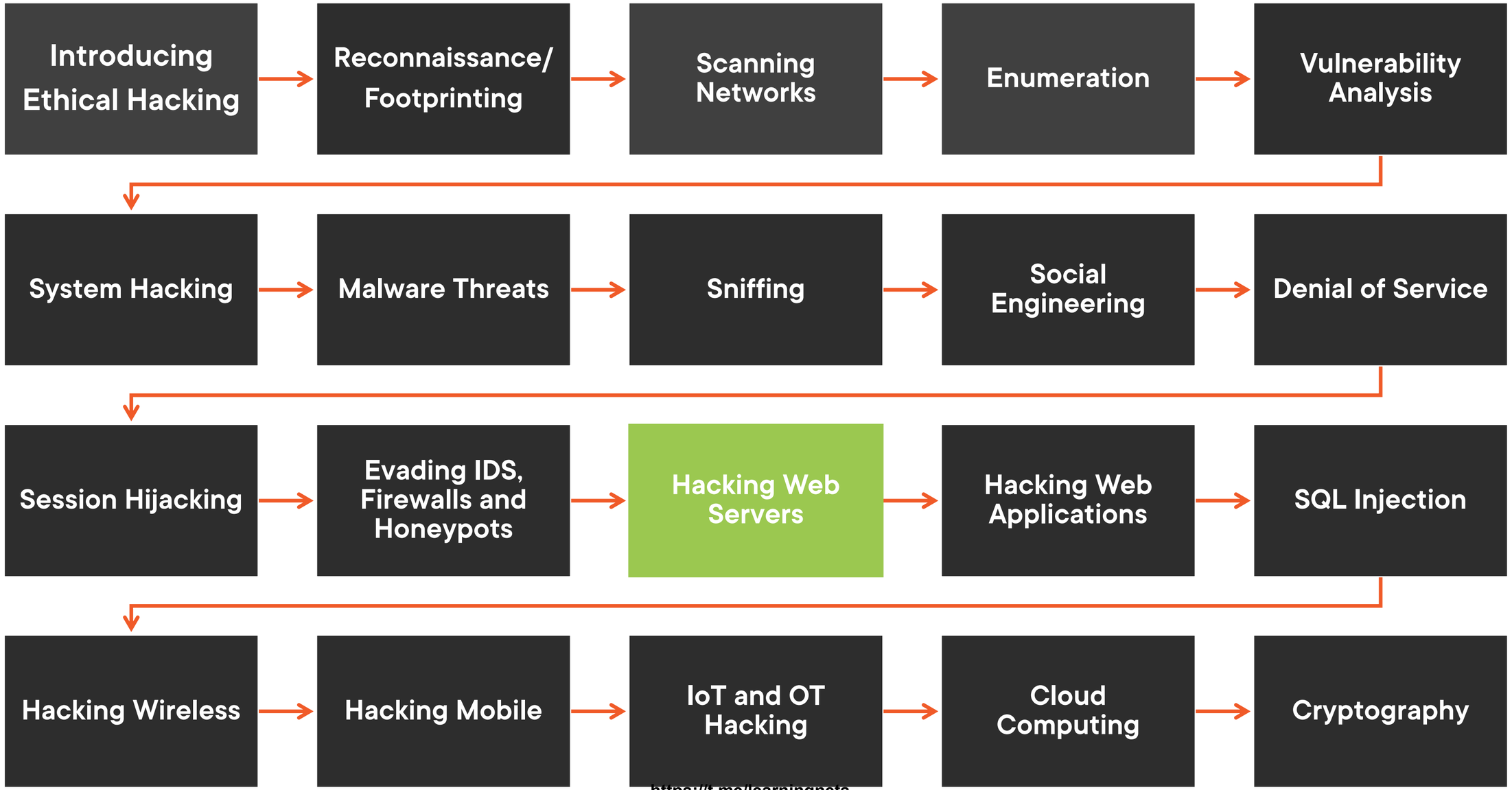
Key Learnings

Web server concepts

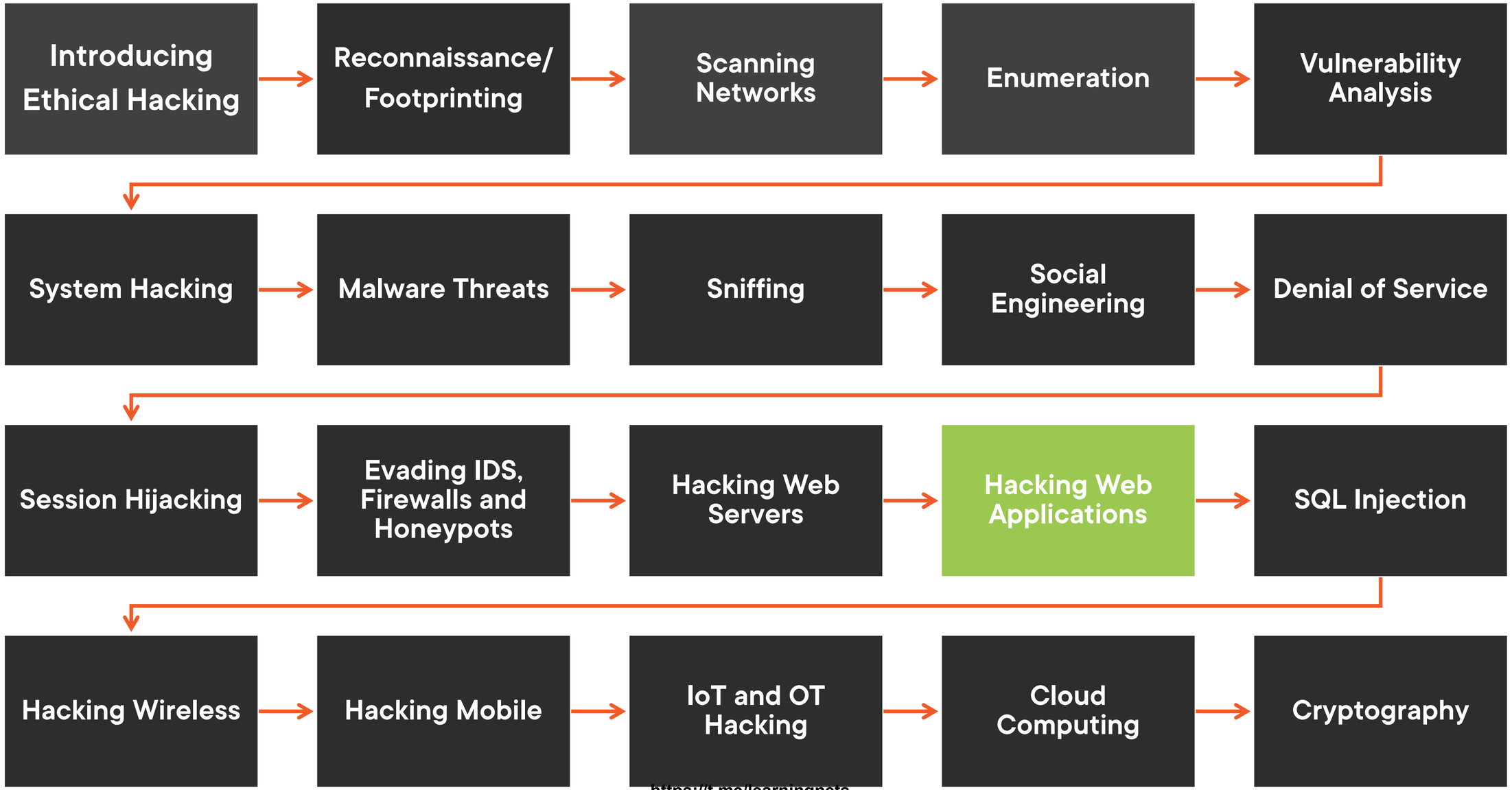
Attack methodology

Web server attacks

Ethical Hacking Series



Ethical Hacking Series



Up Next: How to Hack Web Applications