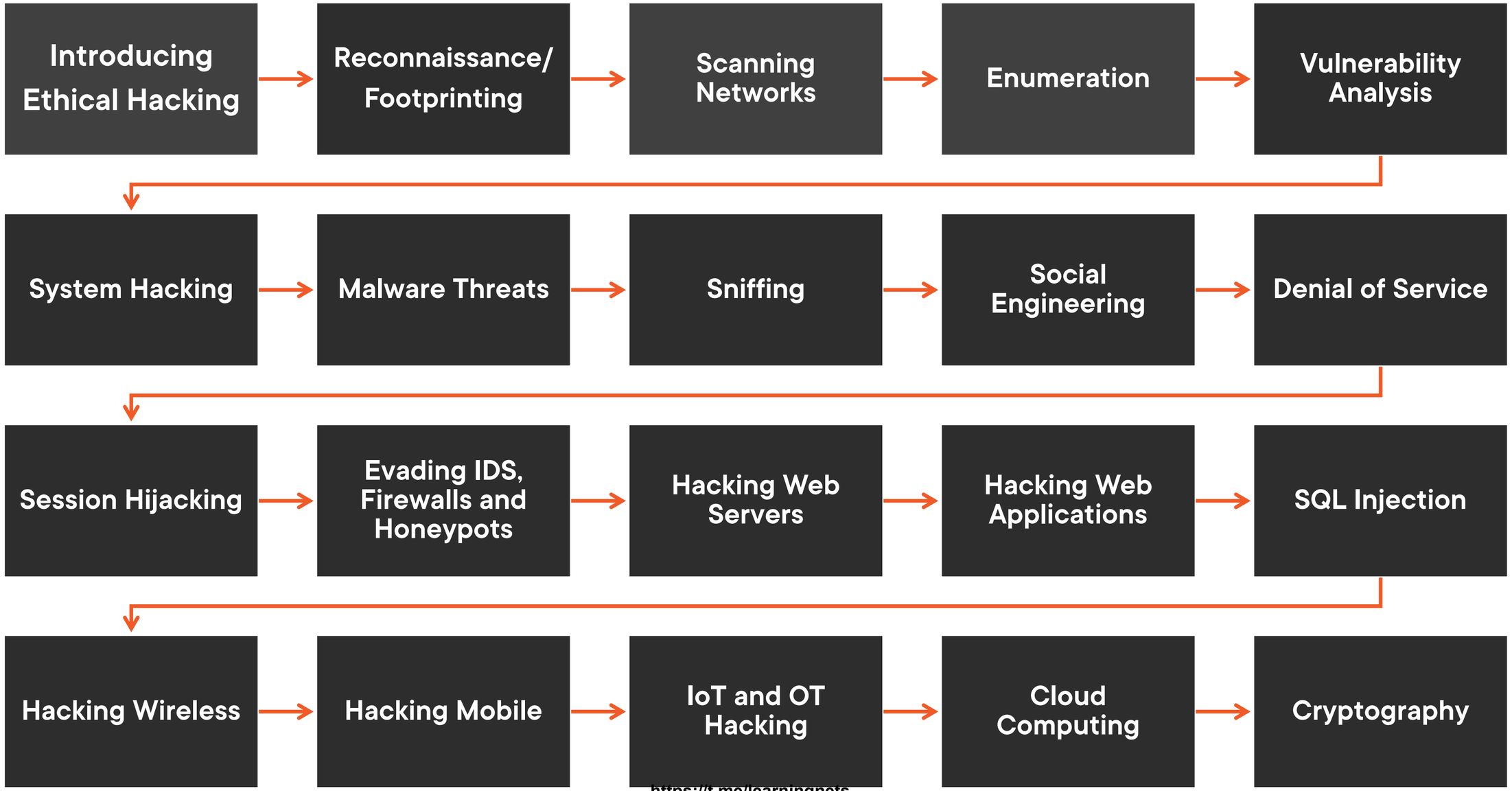
How to Hack Web Applications

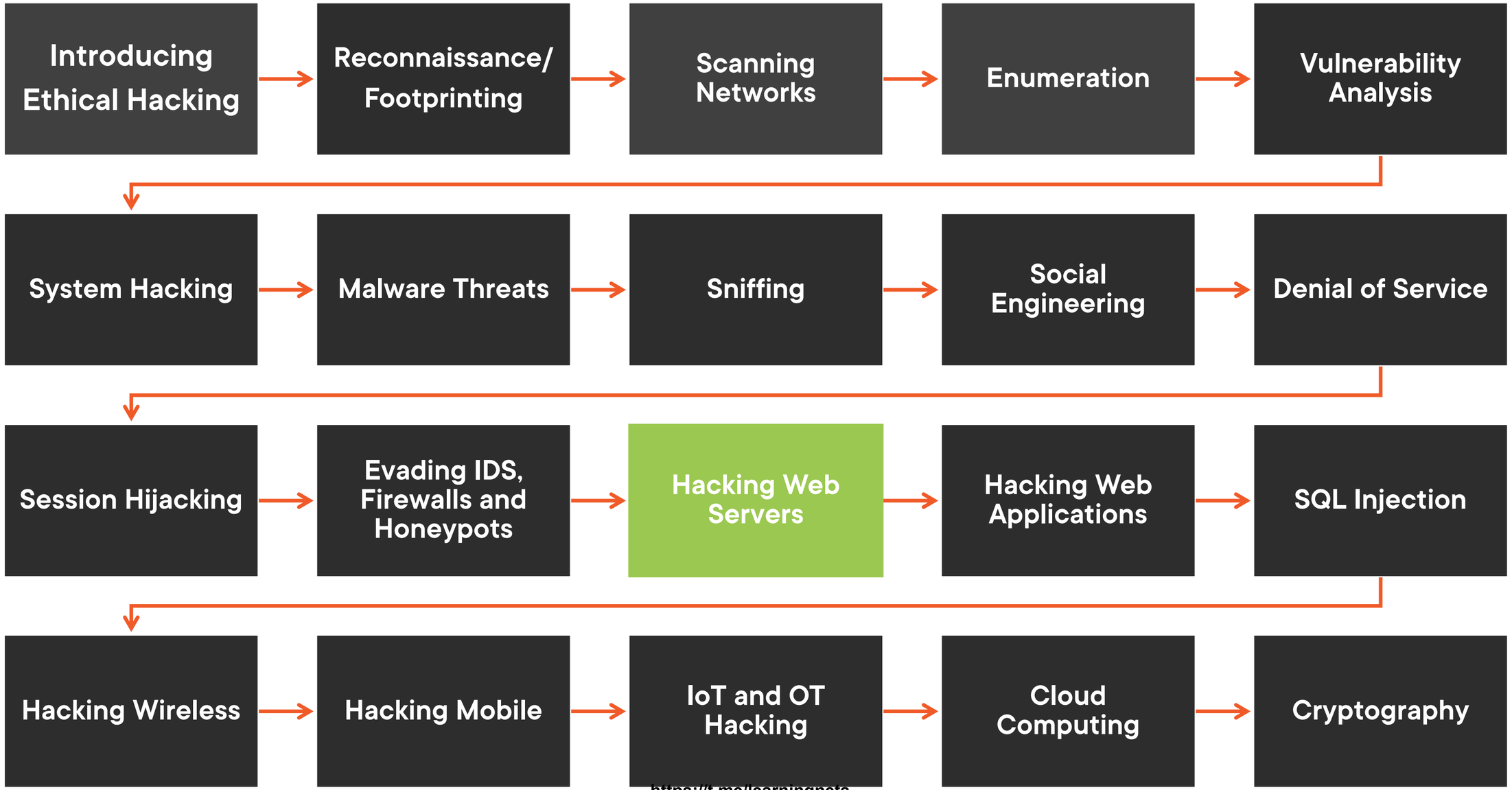
Peter Mosmans
Lead Penetration Tester

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

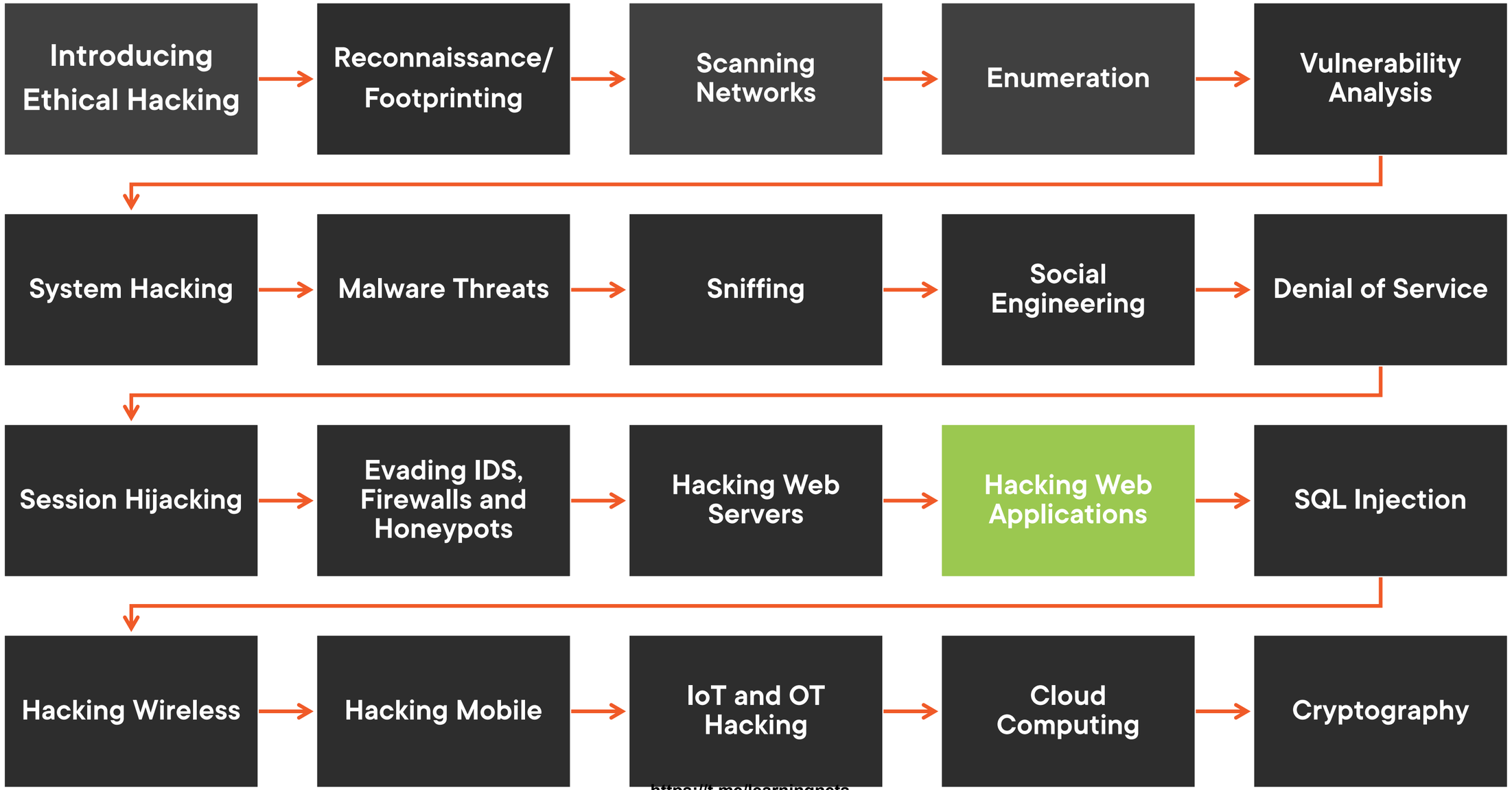
Ethical Hacking Series



Ethical Hacking Series



Ethical Hacking Series



Hacking Web Applications

Web application concepts

Web application threats

Attack methodology

- **Intercepting proxy server**

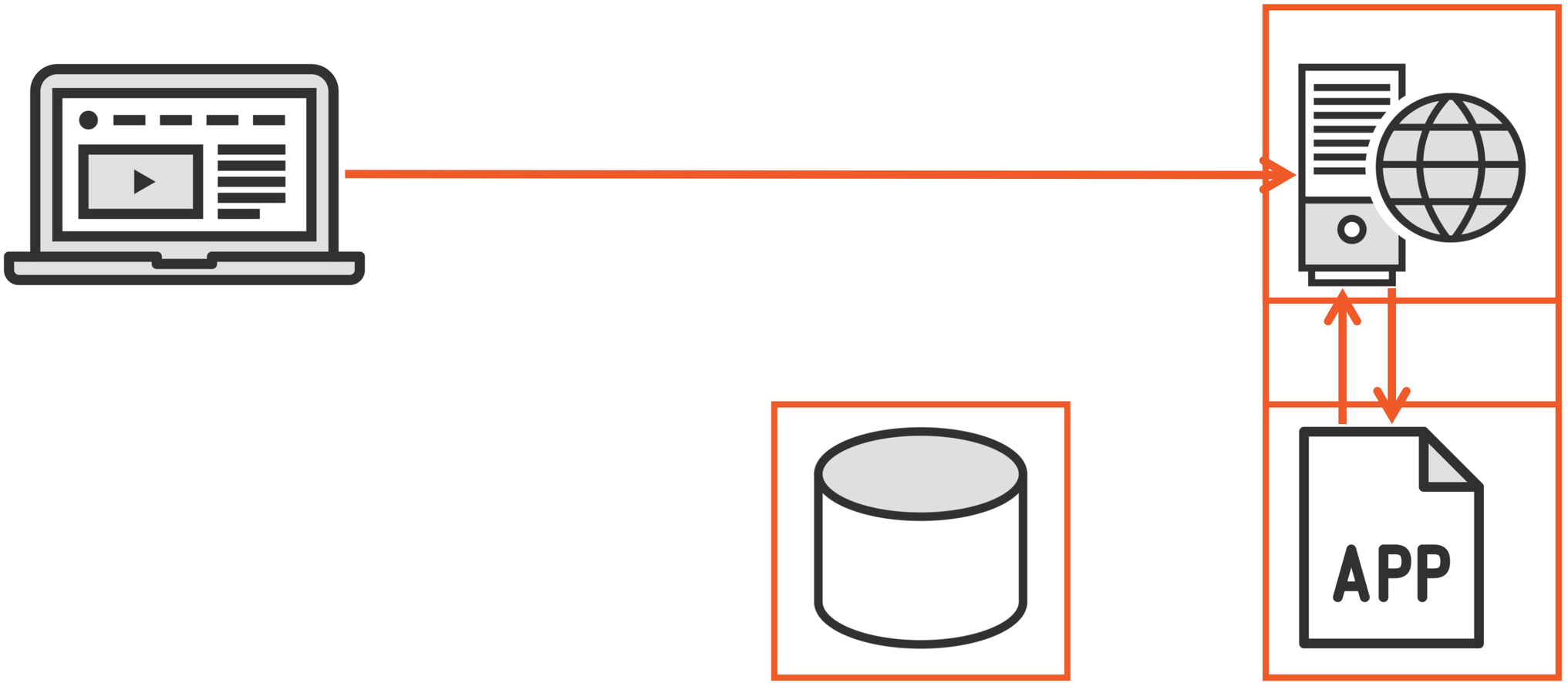
Web APIs

Webhooks and web shells

Web application attack countermeasures

Web Application Concepts

Web Application



Web Application Concepts

Application running on a (different) server

Is available for clients

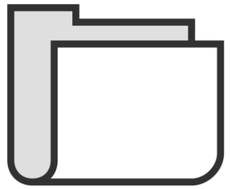
Often accessible 'directly' (HTML)...

...as well as by Application Programming Interface (API)

Web server is responsible for connection

Terminology

Encoding schemes > >



URL Encoding ? %3F

Web 2.0

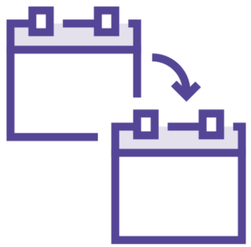
Secure Application Development

Web Application Threats

OWASP Top 10

Open Web Application Security Project

A list of the 10 most critical web application security risks



One 'every 3 years'; Most recent one from 2021; Previous one from 2017

OWASP Top 10 2021

Broken Access Control

Cryptographic Failures

Injection

Insecure Design

Security Misconfiguration

Vulnerable and Outdated Components

Identification and Authentication Failures

Software and Data Integrity Failures

Security Logging and Monitoring Failures

Server-Side Request Forgery

OWASP Top 10 2017

Injection

Broken Authentication

Sensitive Data Exposure

XML External Entities

Broken Access Control

Security Misconfiguration

Cross-Site Scripting

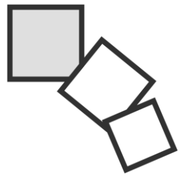
Insecure Deserialization

Using Components with Known Vulnerabilities

Insufficient Logging & Monitoring

Web Application Attacks

Cross-Site Scripting (XSS)



Parameter tampering

Privilege escalation

Insecure Direct Object References (IDOR)

SQL injection attacks

Attack Methodology

Attack Methodology

- Web application information gathering
- Identifying entry points
- Bypassing client-side controls
- Vulnerability scanning
- Exploiting vulnerabilities

Application

Analysis

Client-side controls

Access controls

Authentication mechanisms

Session management mechanisms

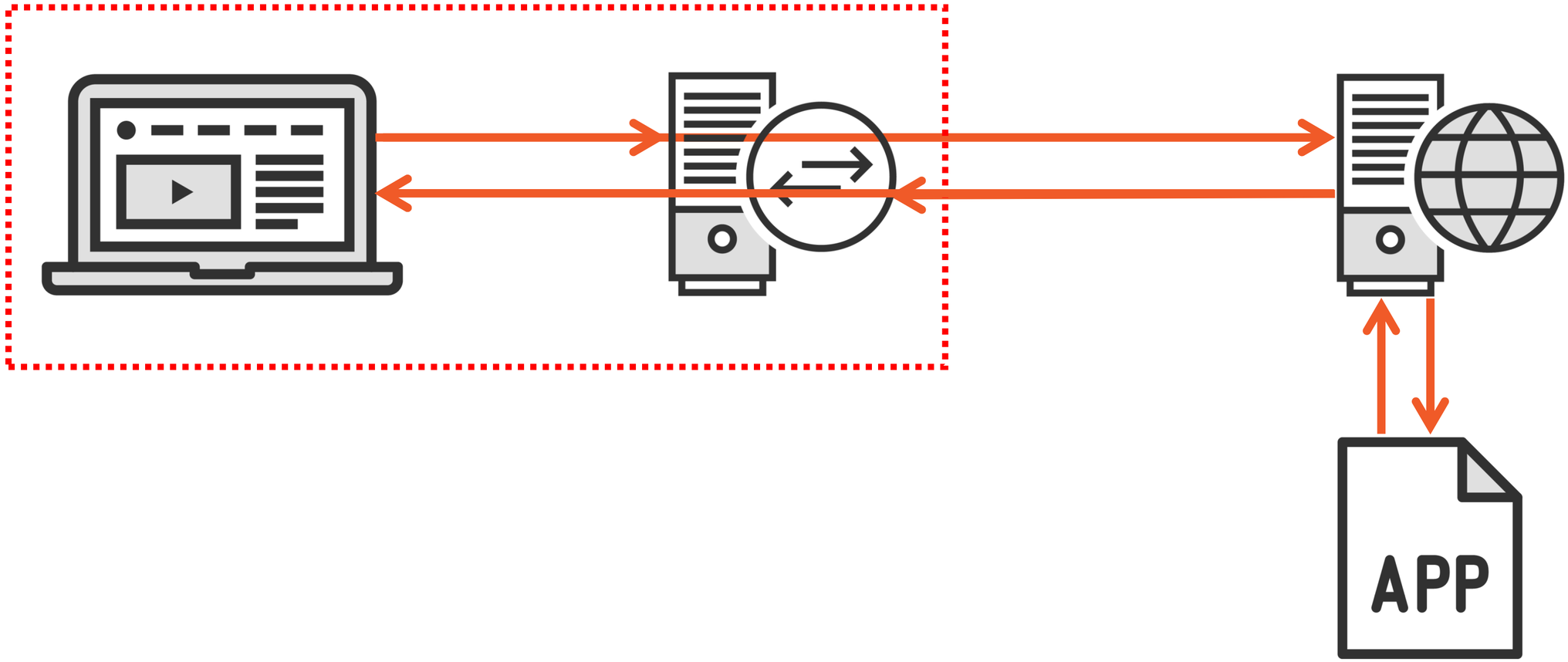
Authorization schemes

Shared environments

Application logic

Database credentials

Intercepting Proxy Server



Web Application Attack Tools

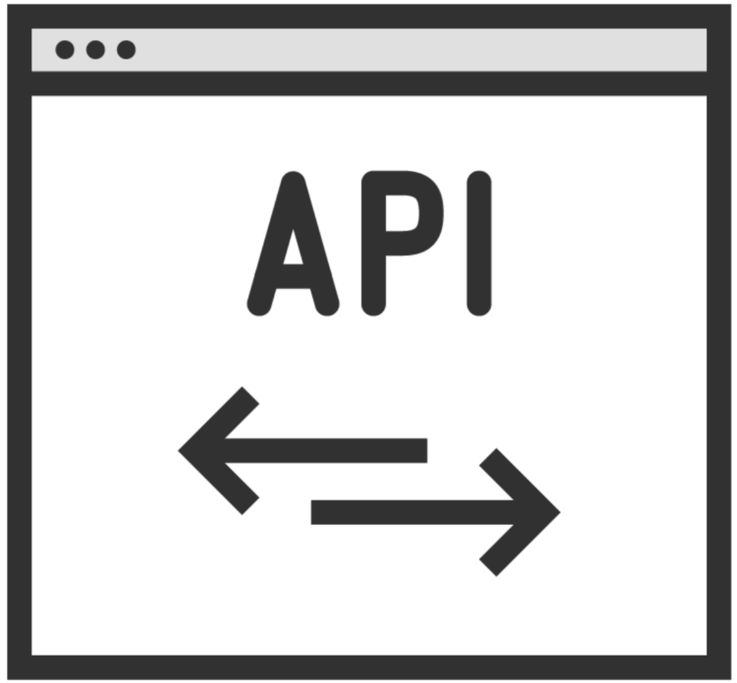
Burp Suite

OWASP ZAP

OpenVAS

Web APIs

Web API



Application Programming Interface

Allows clients to communicate with servers

Set of rules which define the communication

Consumers and producers

Different Protocols and Models

REST API

SOAP API

XML-RPC

JSON-RPC

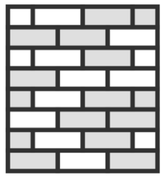
API Attacks and Vulnerabilities

Similar to attacking web applications

Attacking access control

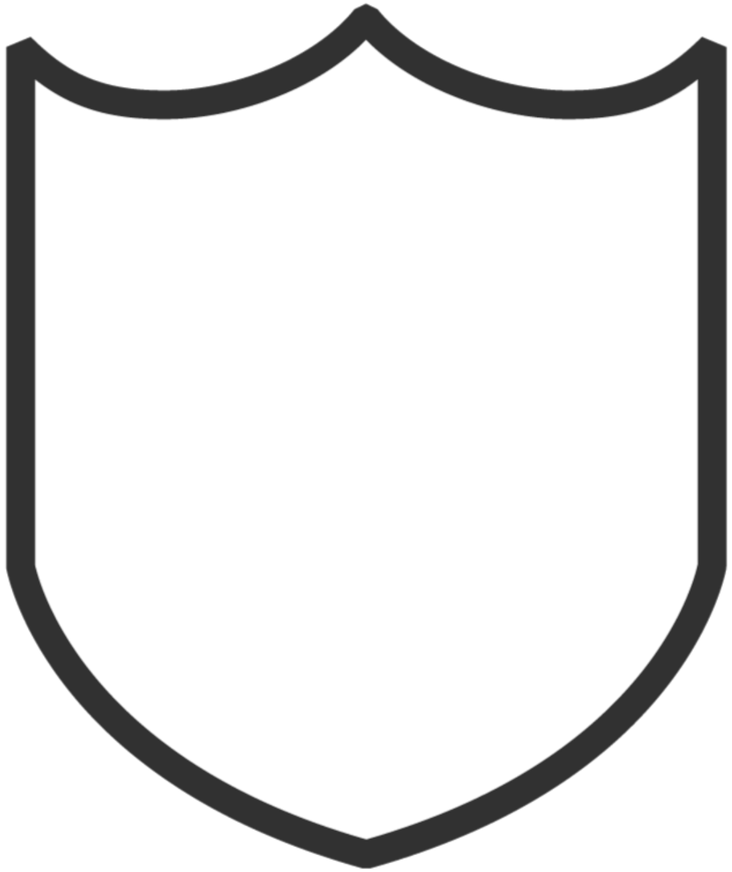
Attacking authorization

Lack of encryption



Insufficiently hardened

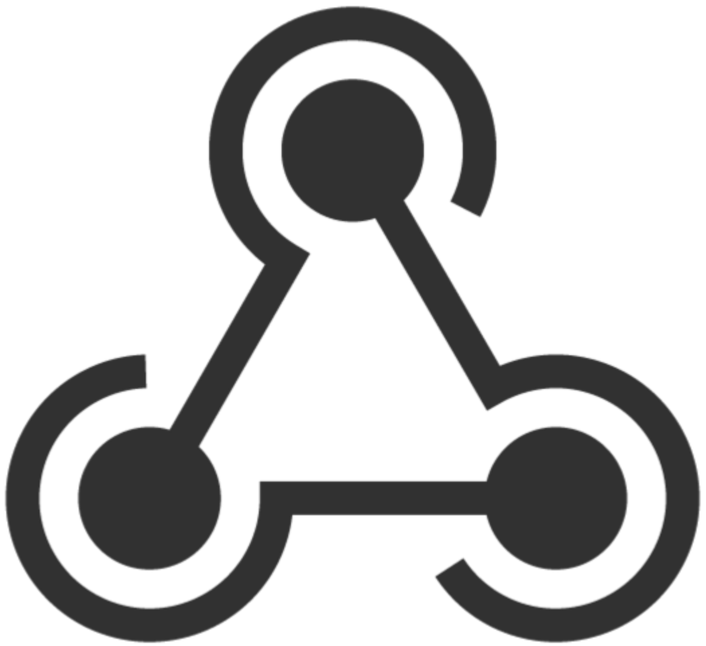
API Attack Countermeasures



- Use transport layer encryption
- Access control
- Whitelisting
- Limit request and body size
- Rate limiting
- Secure coding

Webhooks and Web Shells

Webhooks



HTTP based callback function

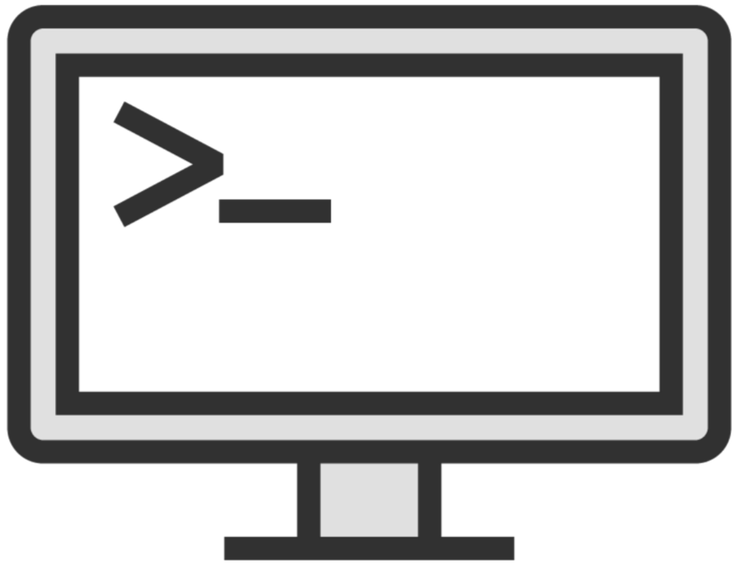
Allows communication between APIs

Event-driven, when events occur

Reverse or push API

Server initiates connection to unique callback address

Web Shells



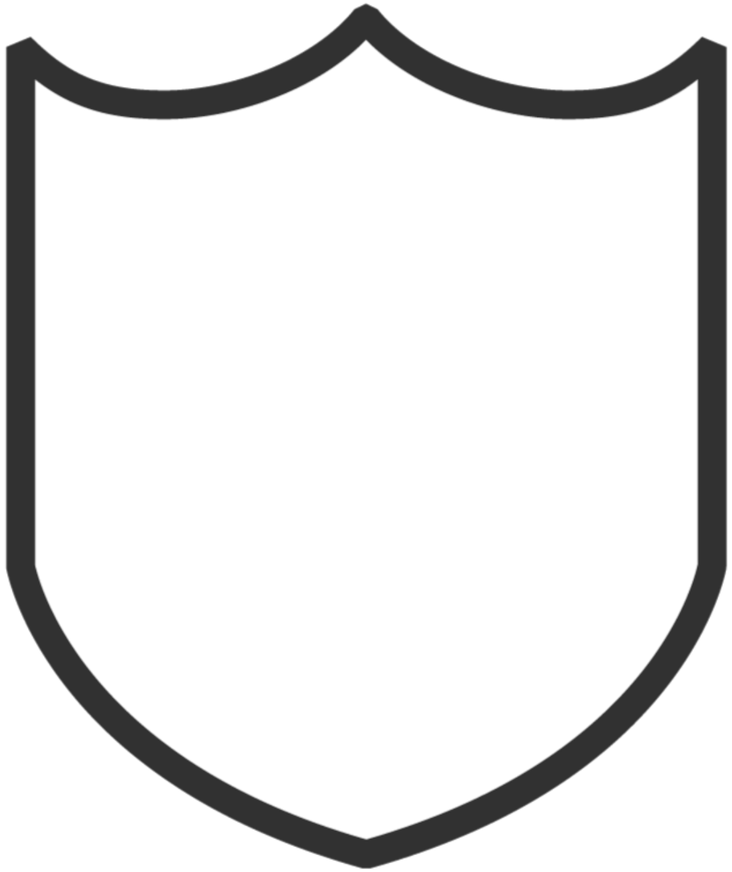
Backdoor, allowing shell access

Using HTTP transport protocol

Often graphical interface for unfettered access

Web Application Attack Countermeasures

Web Application Attack Countermeasures



Implement secure coding practices

Patch management

Check logfiles

Learning Check

Learning Check

- On a remote application server
- Denial of service attack
- Throttling
- Server
- Web shell

Module Review

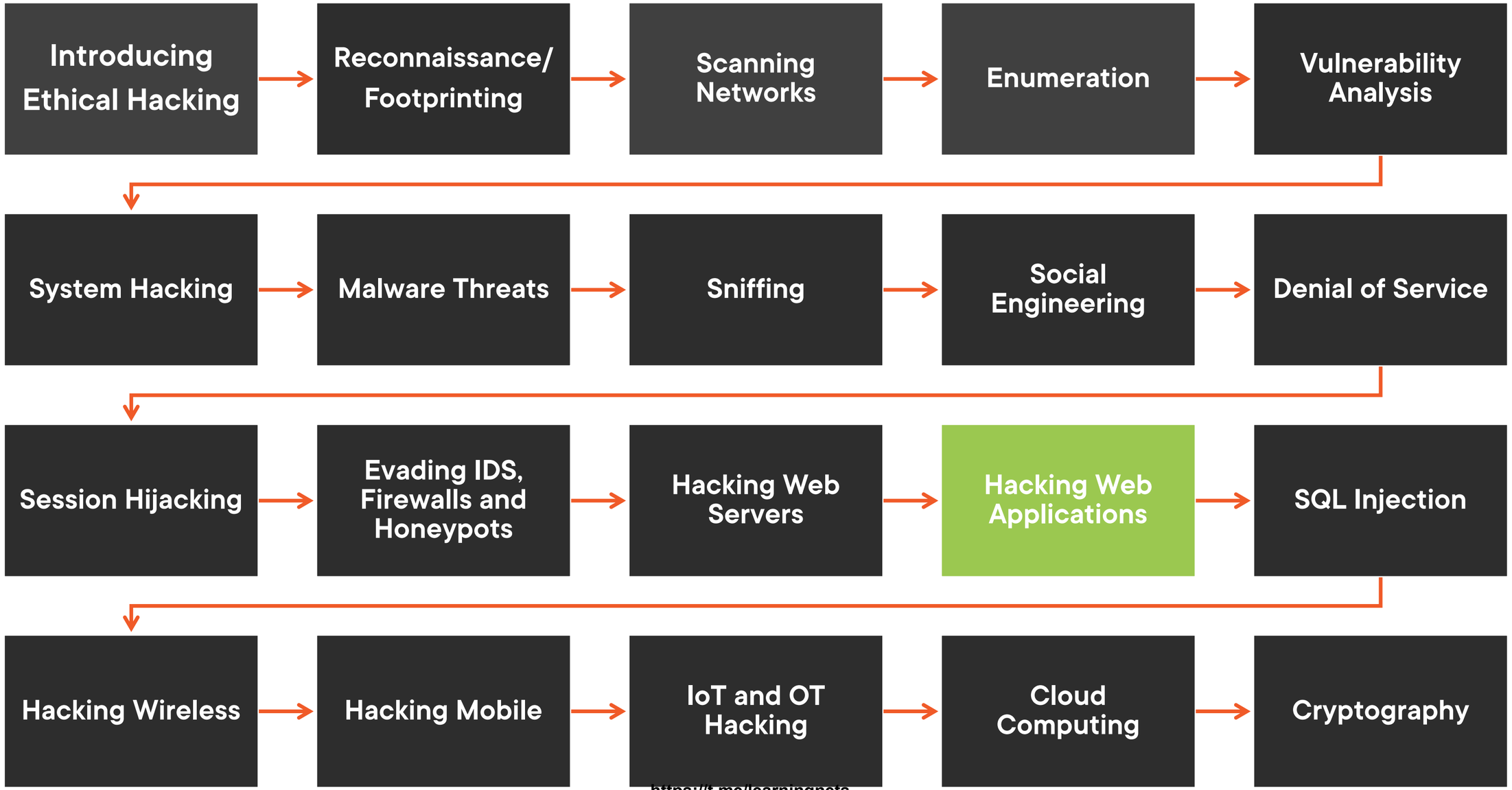
Key Learnings

Web application concepts

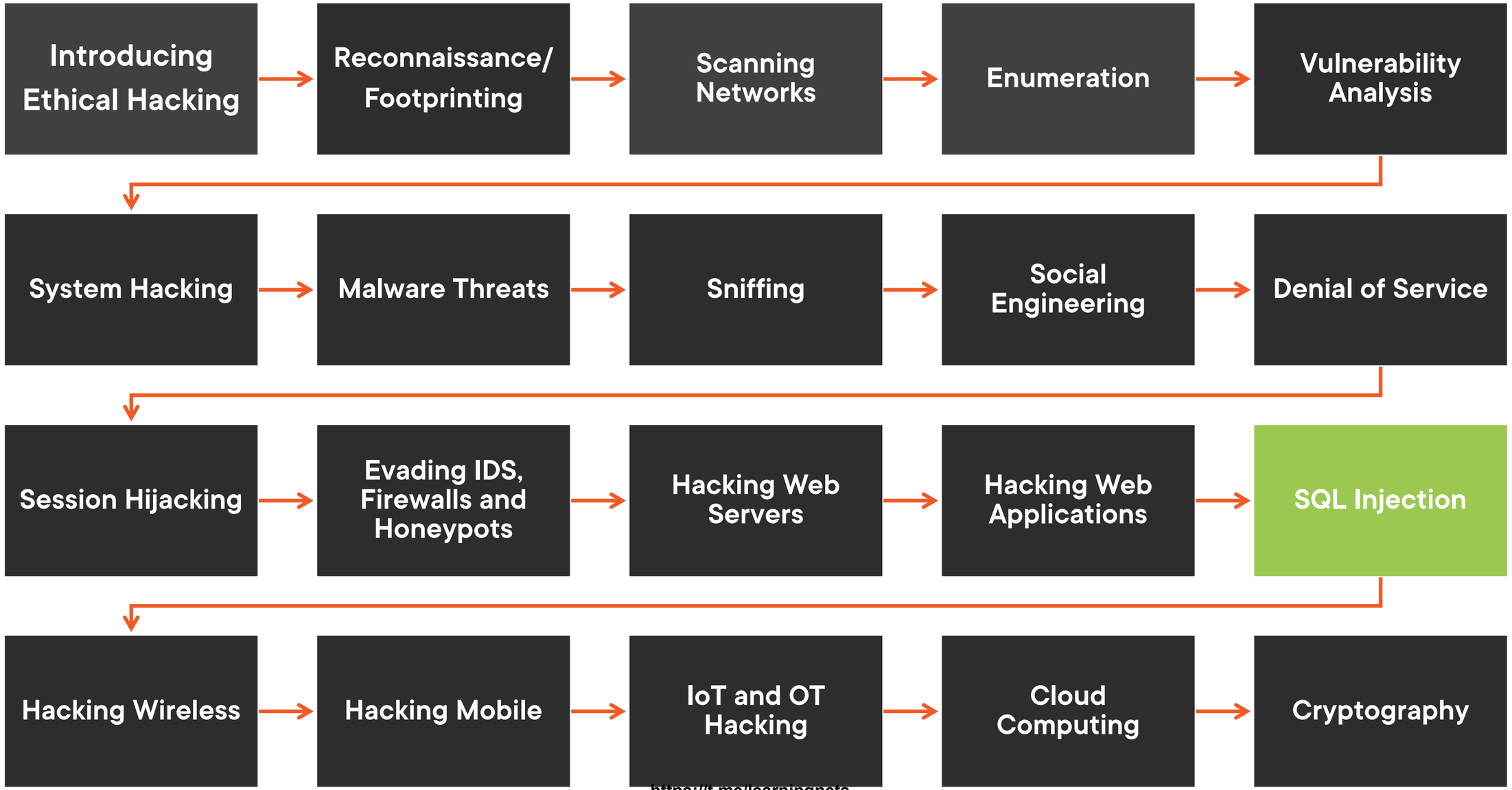
Web application threats

Web application attacks

Ethical Hacking Series



Ethical Hacking Series



Up Next: How to Perform SQL Injection