Ethical Hacking: Social Engineering

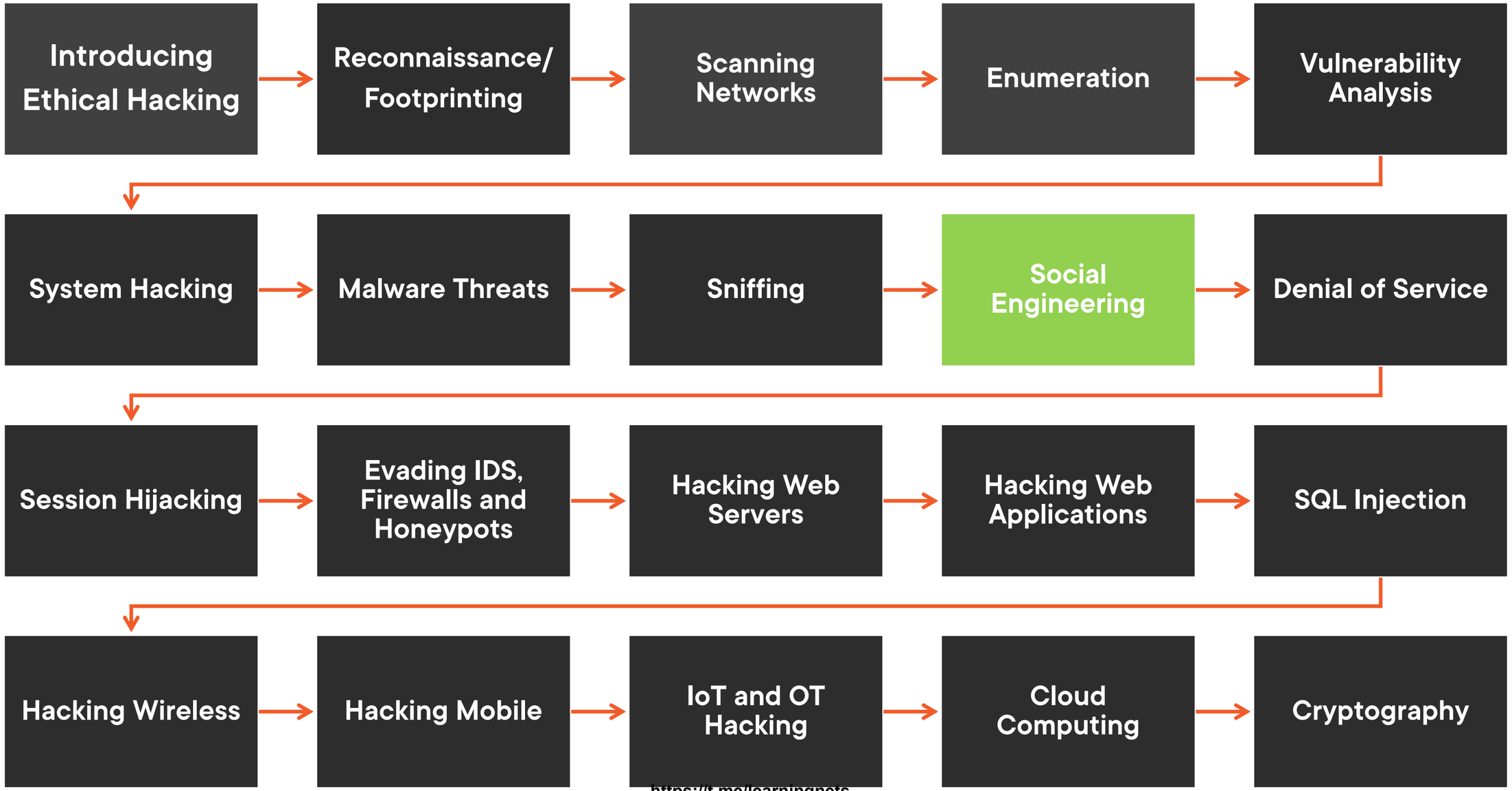
Social Engineering

Alexander Tushinsky

Cybersecurity & Software Development Consultant

@ltmodcs alextushinsky.com

Ethical Hacking Series



Social Engineering

Social Engineering Concepts

- Definition
- Why does it work?

Social Engineering Techniques

- Pretexting
- Attack vectors
- Physical attacks

Social Engineering Concepts

Data Breaches

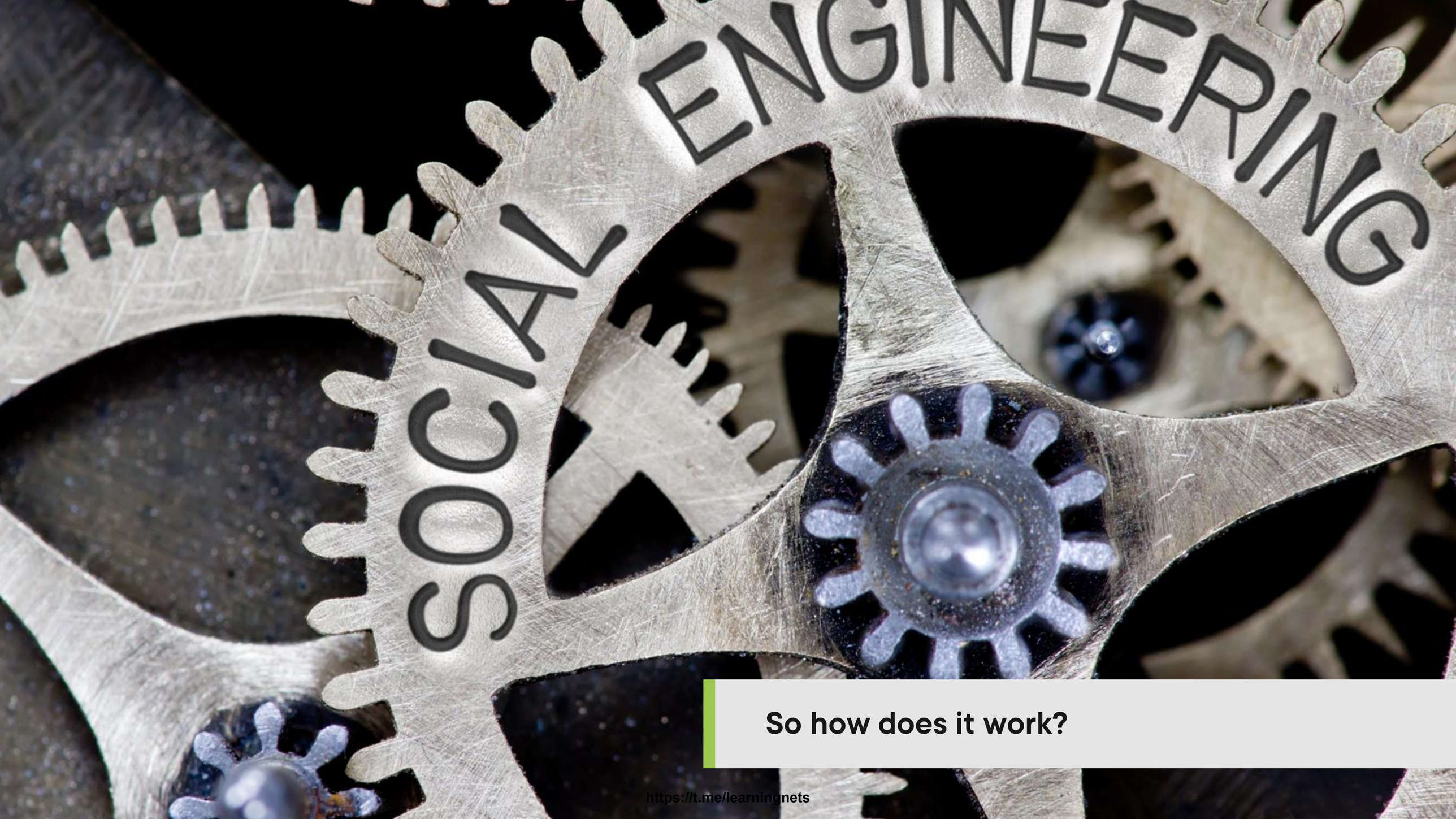
25% - Human Error

27% - Process Failure

80% - Involve Social Engineering

Social Engineering

The art of manipulating an individual or a group of individuals into performing actions that they normally wouldn't perform or divulging information they typically wouldn't provide; The art of human manipulation!



So how does it work?

Principles of Social Engineering

Reciprocity

Authority

Commitment

Liking

Social Proof

Scarcity

Ultimately, it's about trust!

Social Engineering Techniques

Phases of Attack

Research: Gather details about the organization and possible targets you're about to engage with. Techniques here include passive reconnaissance, dumpster diving, and use of Open-Source Intelligence.

Choose a Target: Choose who you feel will be the best target or set of targets for you to achieve your goal.

Pretext: Using a pretext, attempt to build a relationship with the target. This helps build trust.

Exploit: Exploit the relationship to obtain the needed information.

Pretexting

The story you present to the target as the reason for engaging with them.

Pretexting

The script

- Identify how the target will help us achieve our goal
- The pretext helps you achieve the goal
- Identify a “hook” to be used in the exploit phase
- Use the concepts such as liking or reciprocity to further your goal and gain the trust

Attack Vectors

Phishing: Acquire information through deception using digital communication such as email, instant messenger, or social networks.

Vishing: Voice phishing! Uses phone calls to collect information or reconnaissance.

Smishing: Phishing via SMS.

Impersonation: Pretending to be someone you are not to elicit information from a target. A website can be impersonated as well. This rogue site can then be used to collect data.

Demo

Attack Vectors in Action

- Phishing email
- Using WinHTTrack to clone a website

Physical Social Engineering

Physical Access

- Information may be viewable or audible
- Possible access to a data center or network closet
- People may be more inclined to talk to you in person
- Access to a PC may be possible

Attack Vectors

- Tailgating or Piggybacking
- RFID Cloning
- Shoulder Surfing or Eavesdropping
- Dumpster Diving
- Impersonation
- Baiting

Learning Check

Learning Check

- **Reciprocity**
- **Pretext**
- **Phishing**
- **Dumpster Diving**

Module Review

Key Learnings

Social Engineering Concepts

Social Engineering Techniques

Explored Impersonation

Up Next:
Consequences and Countermeasures