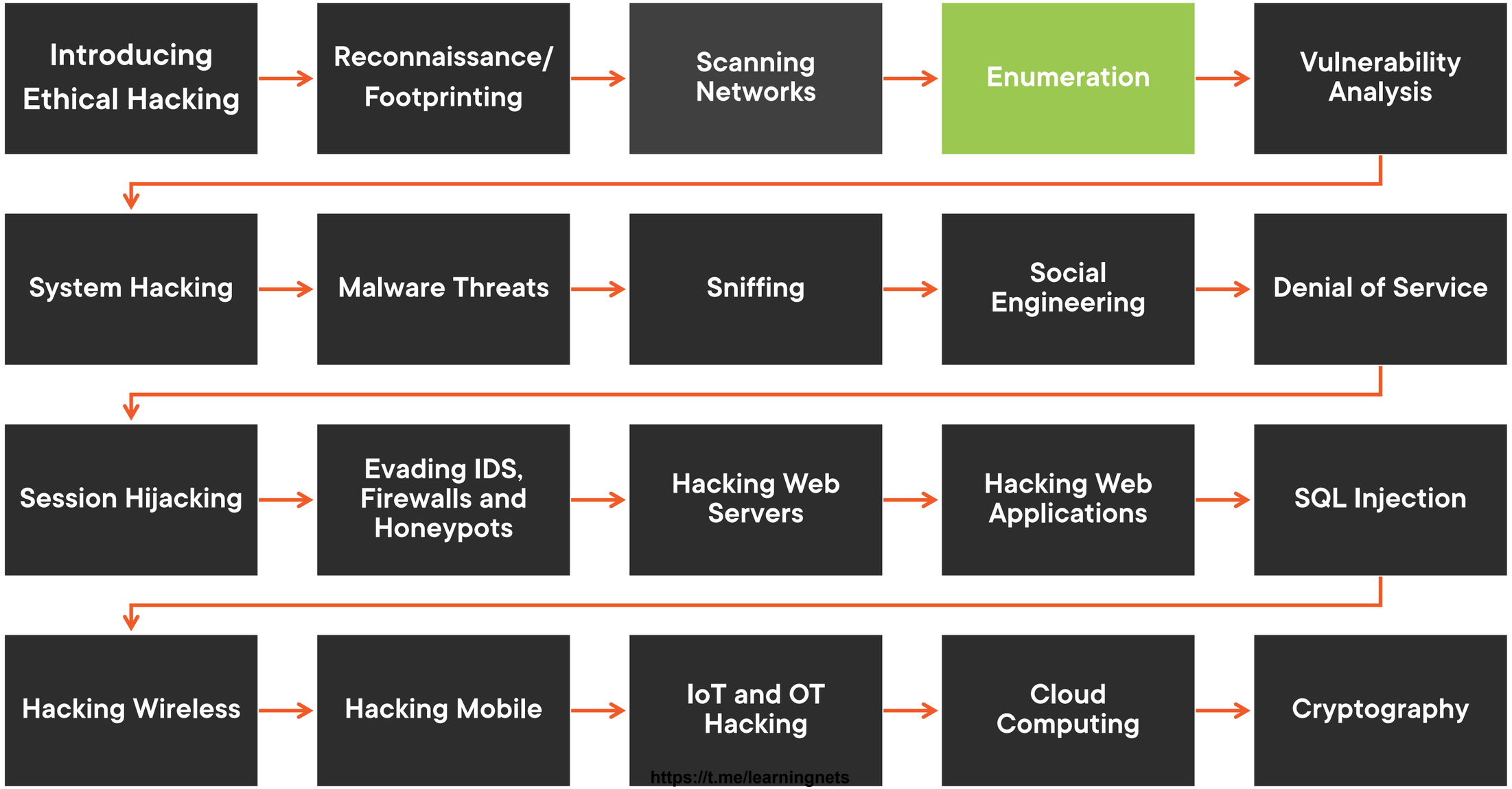
Ethical Hacking: Enumeration

Discussing Enumeration and the Techniques Used

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Ethical Hacking Series



Lab/Demo Environments

Online:
Pluralsight Labs

Virtual:
“Building a Cybersecurity Home Lab Environment”

Enumeration Explained

A lot of hacking is playing with other people, you know, getting them to do strange things.

Steve Wozniak

Explaining Enumeration

Usually conducted internally

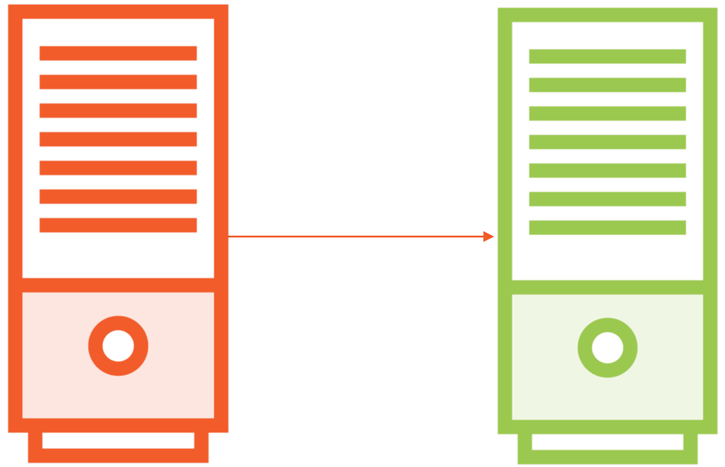
Requires an active connection

Attacker then directly queries the target

Looks for remote IPC$ shares

Looks for services that offer up data

Create a Null Session



Explaining Enumeration

Looking at what a target exposes:

- **Usernames**
- **Groups**
- **Machine names**
- **Network resources**
- **Services running**

Explaining Enumeration

Looking at what a target exposes:

- **Routing tables**
- **Auditing services**
- **Applications**
- **DNS & SNMP info**

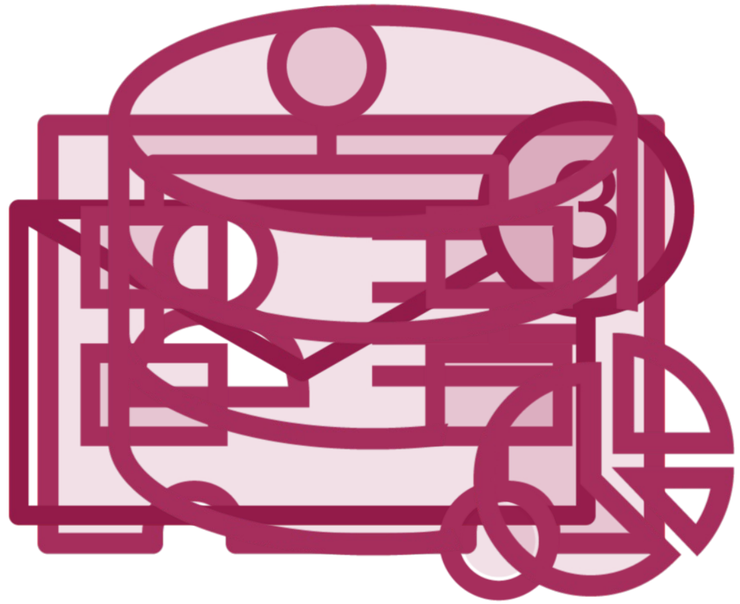
The Techniques of Enumeration

Possible Weaknesses

Email information or a business card

Windows groups

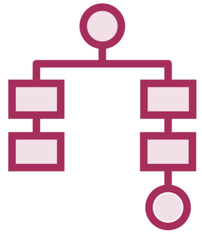
DNS zone transfers



Possible Weaknesses

Email information or a business card

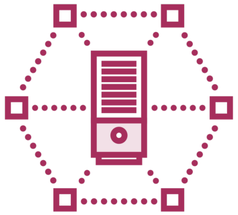
Brute force Active Directory



Windows groups

Default passwords

DNS zone transfers



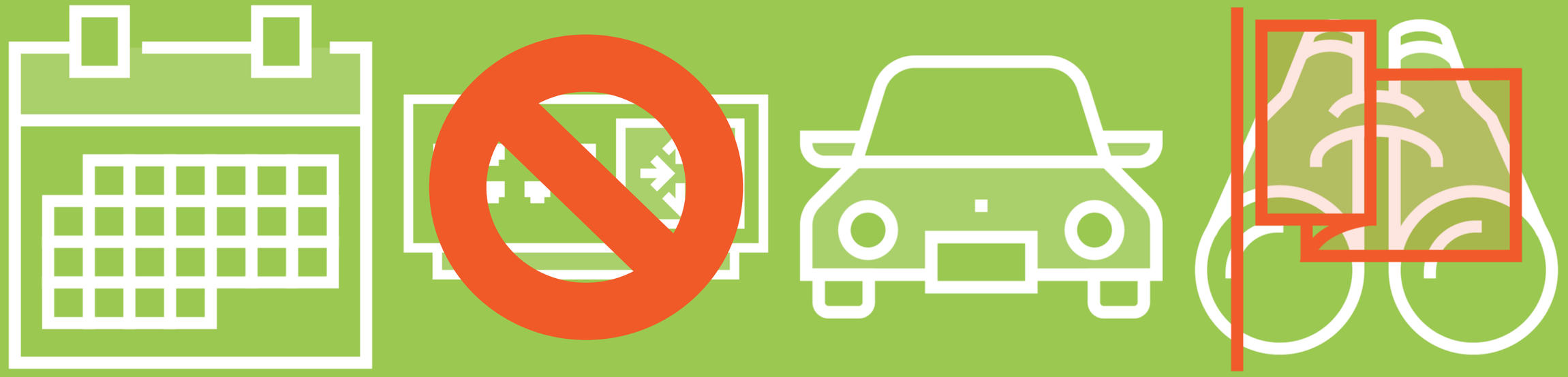
SNMP

Know Your Ports and Services

Know Your Ports and Services

DNS zone transfers	SMTP	MS RPC Endpoint	Global Catalog Service	NetBIOS Naming Service
• TCP 53	• TCP 25	• TCP 135	• TCP 3268	• TCP/UDP 137

LDAP	SMB over NetBIOS	SNMP	SMB over TCP
• TCP/UDP 389	• TCP 139	• UDP 161	• TCP 445



Learning Check

Learning Check

- **Business card**
- **Port 25**
- **Port 3268**
- **Port 53**

Up Next: Enumerating via Defaults & NetBIOS