Clearing Logs – Covering Your Tracks

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

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

These are not the droids you're looking for.

Obi-Wan Kenobi

Why We Cover Our Tracks

Umm...DURRRRR

Remain obscure

Avoid “trace-backs”

Convince “victim(s)”

Basic Methods

A Good Attacker

- Clear browser history
- Delete cookies
- Delete downloads
- Clear password manager
- Delete private data
- Clear logs

Demo

Basic methods of covering your tracks

Advanced Methods

A Great Attacker

Disable auditing

Do damage

Enable auditing

Demo

Advanced methods of covering your tracks

Demo

Covering BASH histories

Learning Check

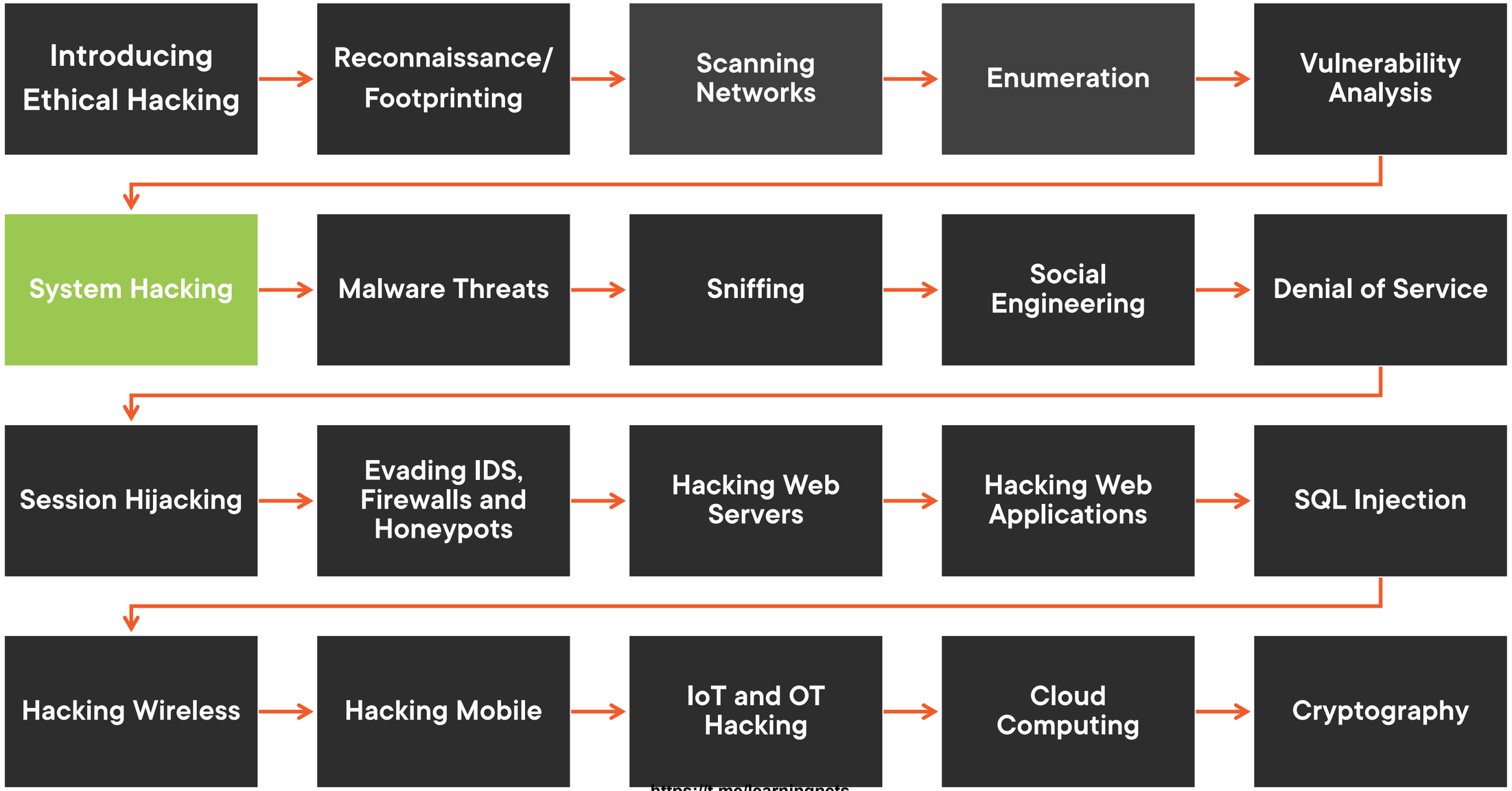
Learning Check

- Trace-backs
- Clear logs
- Disable auditing
- auditpol
- History

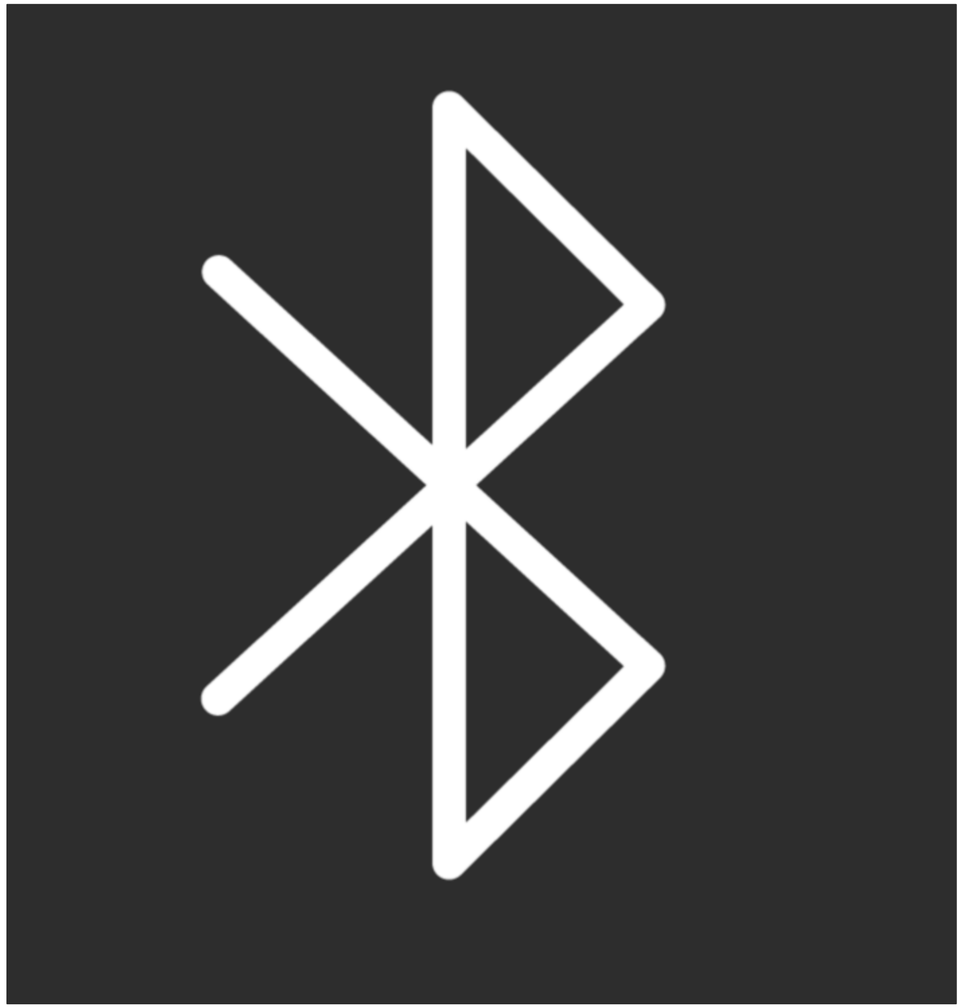
Key Terms

- **Goals**
- **Auditpol**
- **First entry is a delete entry**

Ethical Hacking Series



Connect with Dale



www.dalemeredith.com

Twitter: @dalemeredith

LinkedIn: Dale Meredith

Thanks for watching

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

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