

Examining the Tools of Attackers and the Countermeasures



Dale Meredith

MCT/CEI/CEH/Speaker/Security Dude

Owner: Wayne Technologies

 :@dalemeredith  :daledumbsITdown  :daledumbsITdown

 :dalemeredith www.daledumbsITdown.com

Demo



Using Maltego

Demo



Fire up Recon-ng

Demo



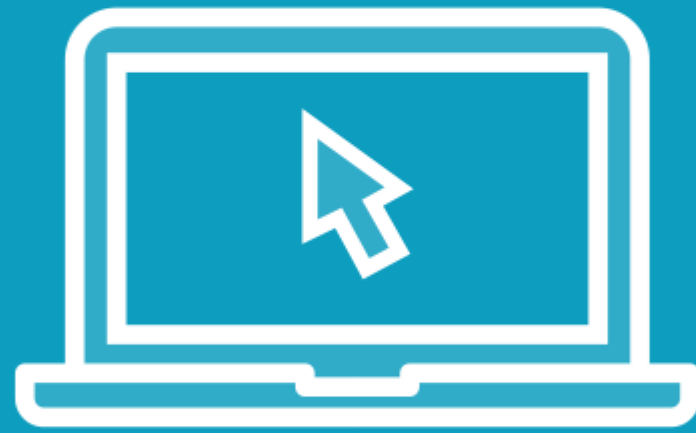
FOCA

Demo



The OSRFramework

Demo



OSINT Framework

What Are the Countermeasures?

Countermeasures

Security policies

Disable directory listings

Offline any critical documents

Training and testing for social engineering attacks

Don't give up locations/travel

Countermeasures

Disable geo-tagging on phones and cameras

Avoid domain-level cross-linking

Use privacy options for WHOIS

Restrict DNS zone transfers

Don't need it, turn it off

Thanks for Watching



Dale Meredith

MCT/CEI/CEH/Speaker/Security Dude

Owner: Wayne Technologies

 :@dalemeredith  :daledumbsITdown  :daledumbsITdown

 :dalemeredith www.daledumbsITdown.com