

Examining WHOIS and DNS for Intel



Dale Meredith

CEH, CEI, MCT, security dude and owner of Wayne Technologies

@dalemeredith

www.daledumbsITdown.com



Whois



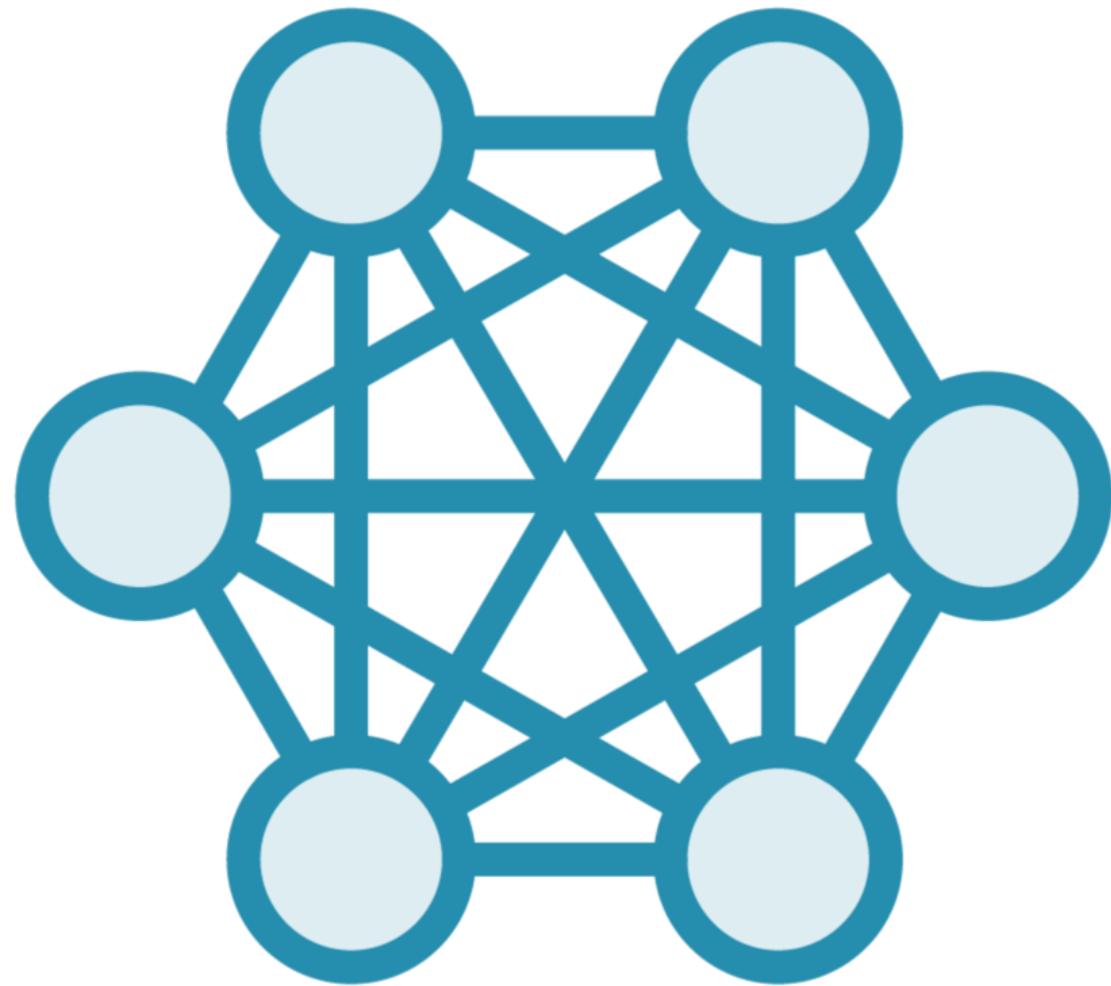


Whois

<https://t.me/learningnets>



Whois



Contact info:

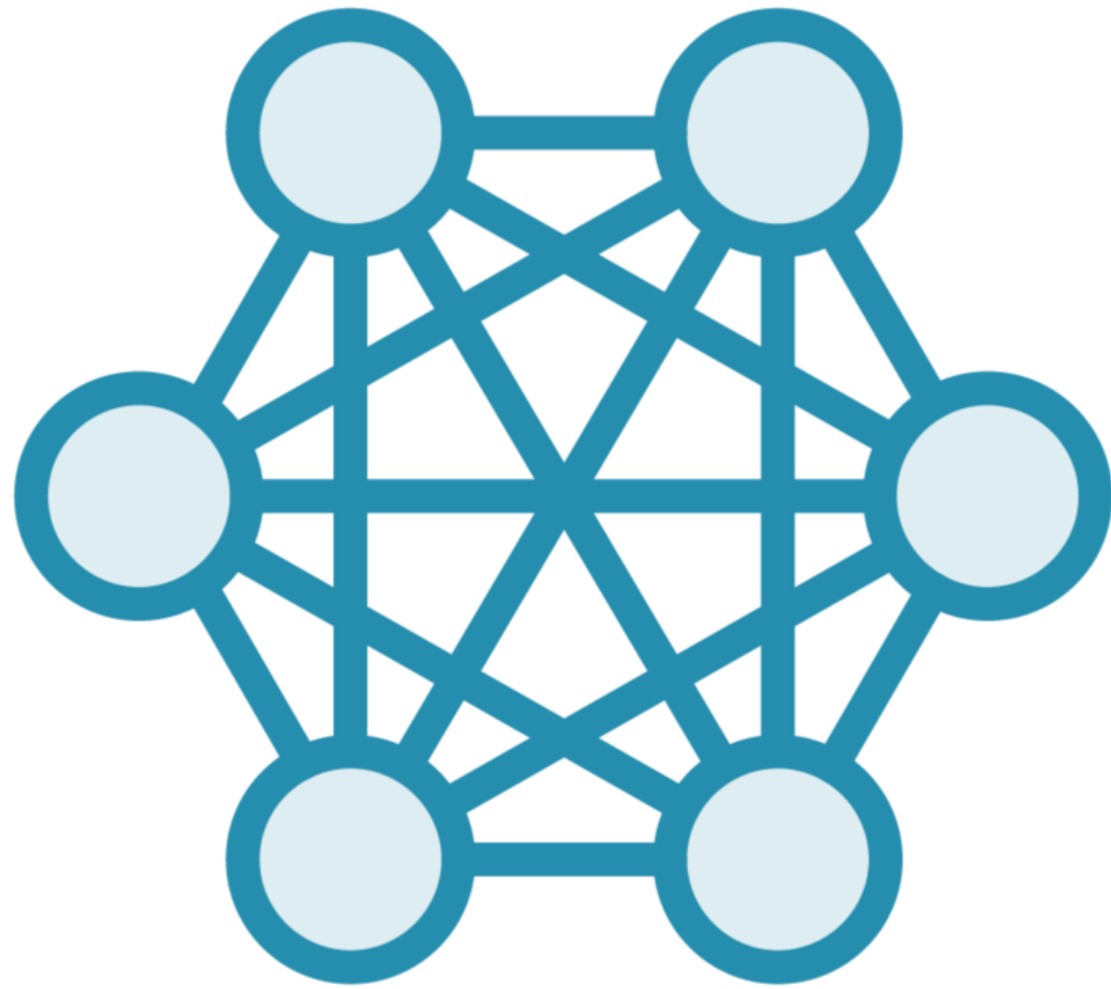
- Domain's registrant
- Registrant organization
- Addresses
- Phone numbers
- Email addresses

Status

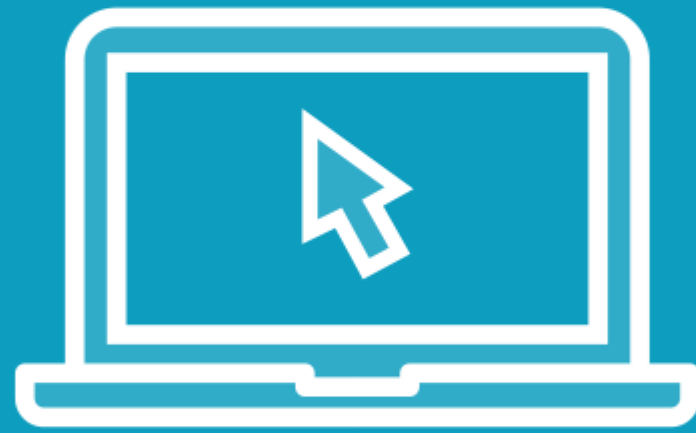
Name servers



Whois



Demo



WHOIS



DNS Footprinting





A / AAAA

CNAME

MX

NS

SOA

TXT

SPF



nslookup
dig
Web apps
Zone transfers



Demo



Using NSLookup



Demo



Using DNSRecon



Certificates



Certificates



Certificates



Subject alternative name (SAN)

Wildcards *

Certificate Transparency (CT)



Up Next:

Discovering Intel from Network
Reconnaissance/Footprinting





Contact info

Twitter: @dalemeredith

Instagram: @daledumbsITdown

YouTube: daledumbITdown

LinkedIn: dalemeredith

Website: daledumbsITdown.com

