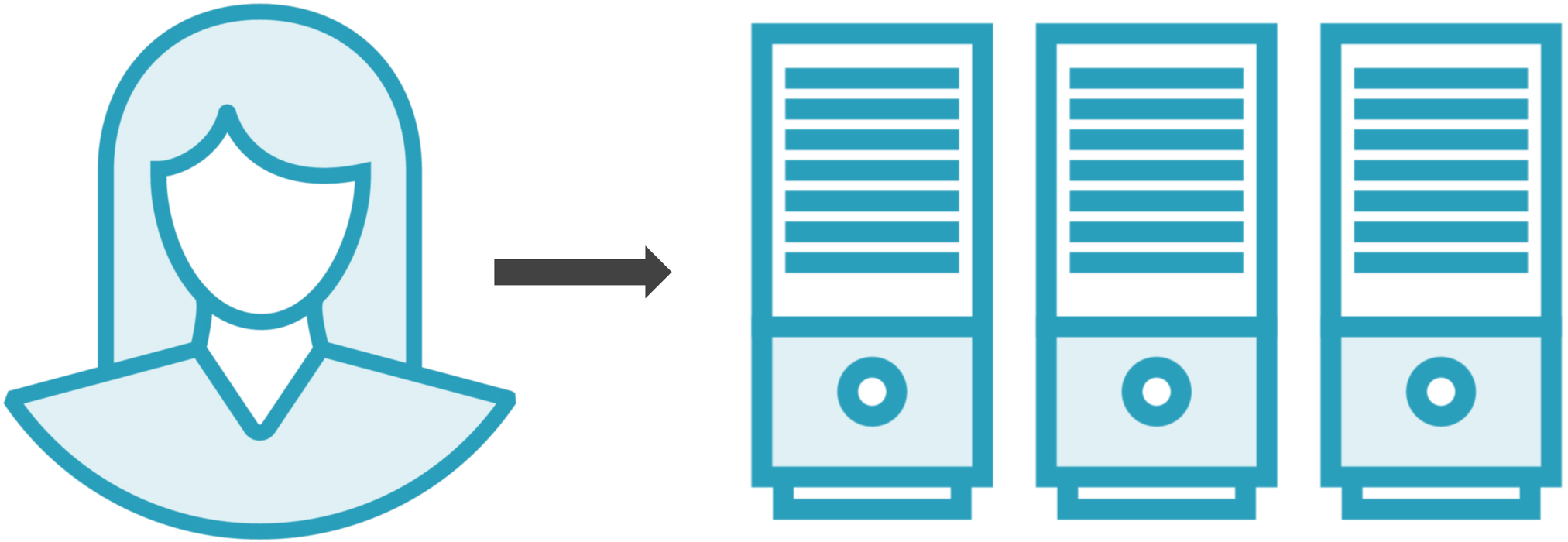
Employing DNS Enumeration

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

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

Domain Name System



What’s in a name?

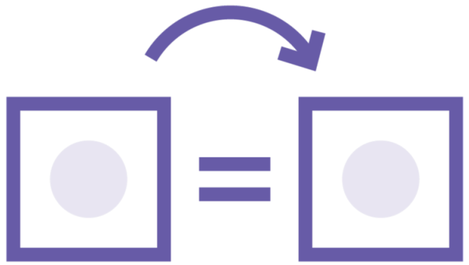
William Shakespeare

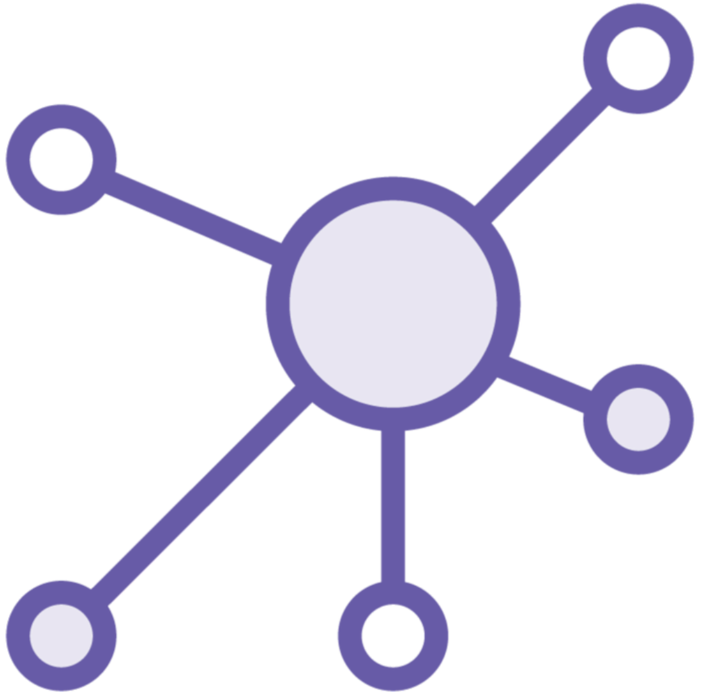
What Is DNS?

IP	Name	Service
192.168.0.1	NY-DC1	LDAP
192.168.0.2	NY-DNS1	SOA

What Is DNS?

- Record lookup
- Cache snooping
- Google lookup
- Reverse lookup
- Zone walking
- Zone transfers





Behind DNS

Behind DNS

Ports

UDP 53 Faster resolution

TCP 53*

Records

A

AAAA

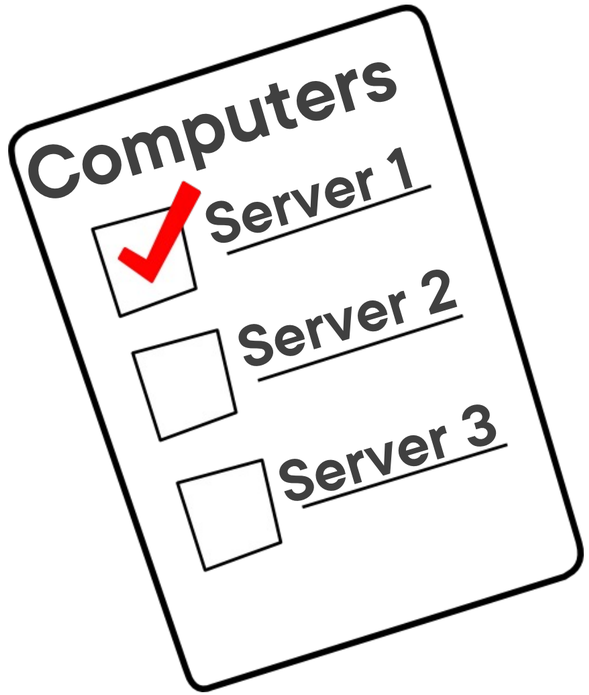
CName

NS

SOA

PTR

Batcave = > 10.10.10.5 | www = > batcave



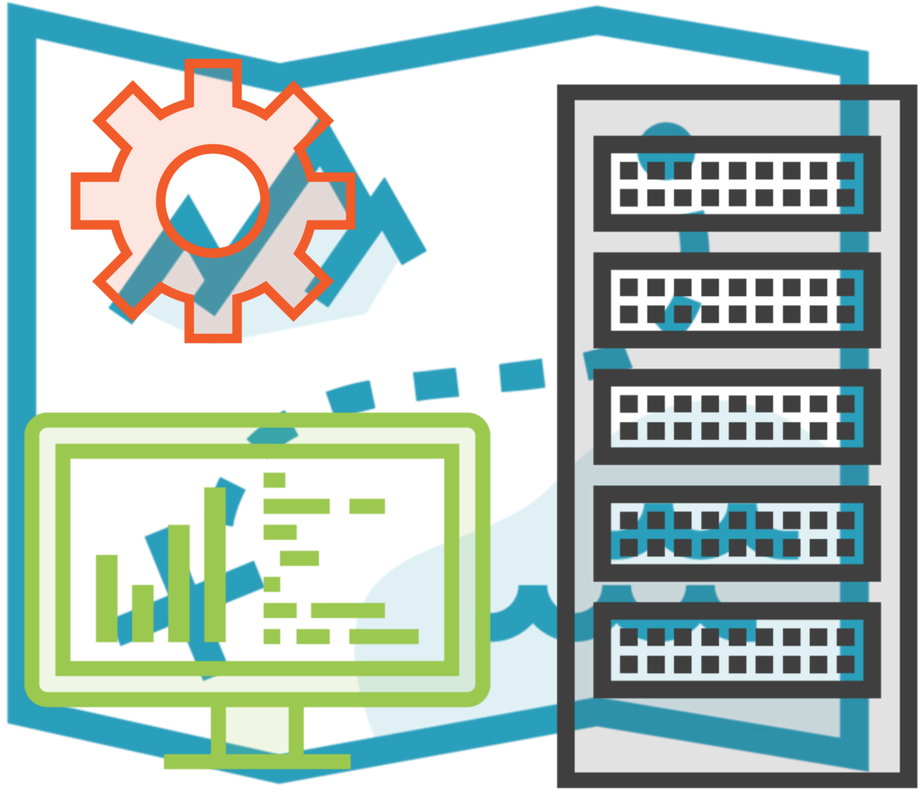
What Can You Learn from DNS?

The Mother load

Servers

Workstations

Services => servers



Demo

Using NSLookup and DNSRecon:

Learning Check

Learning Check

AAAA

MX

SRV

PTR

Up Next: Acquiring Intel from Other Enumeration Techniques