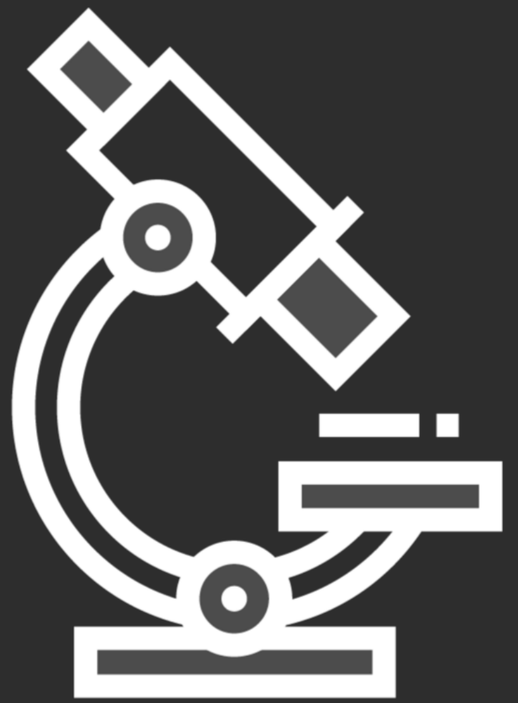
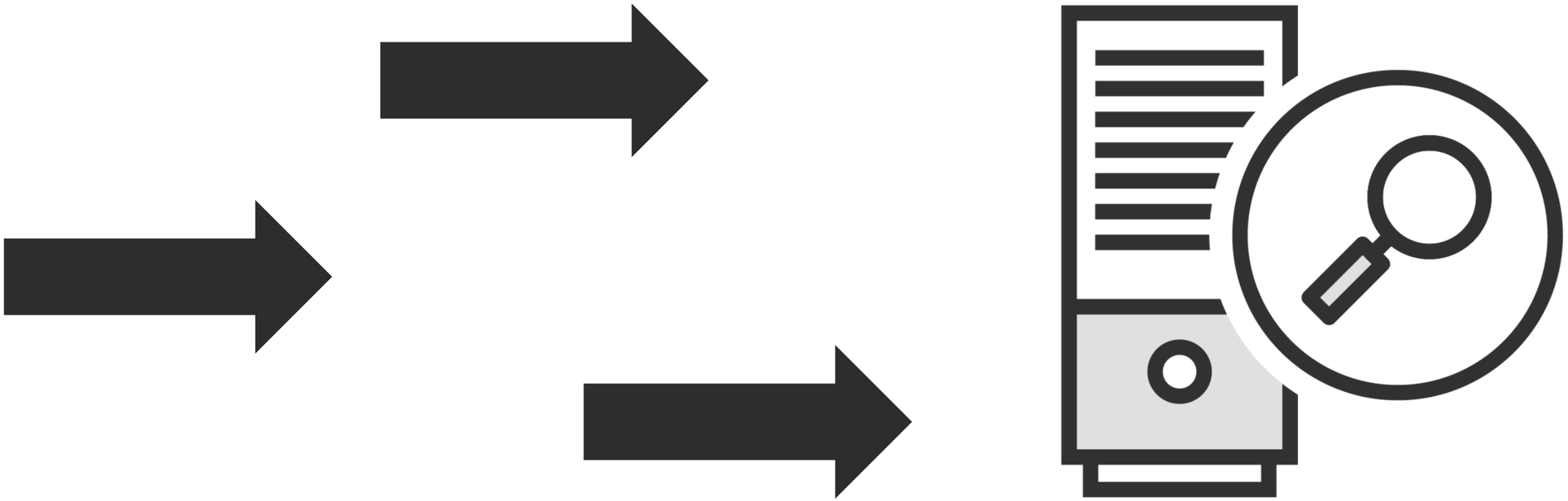
Utilizing Banner Grabbing and OS Fingerprinting

Dale Meredith

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

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





Two Types of Fingerprinting

Active Fingerprinting

Uses specially crafted packets

Reponses are compared to a database of known responses

Extremely high chance of detection

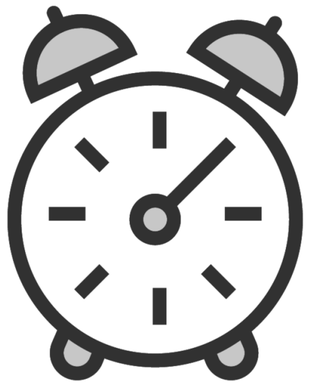
Two Types of Fingerprinting

Active Fingerprinting

Uses specially crafted packets

Reponses are compared to a database of known responses

Extremely high chance of detection

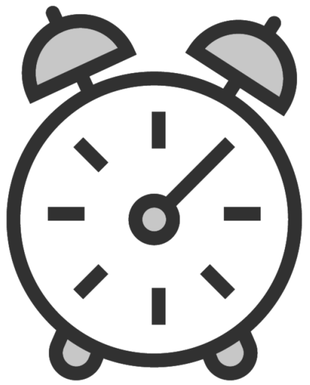


Passive Fingerprinting

Sniffs network traffic

Responses are analyzed to discover any details that could ID the system

Chances of detection are extremely low



Demo

Using Nmap to fingerprint the OS

Banner Grabbing

The Welcome Mat of Computers

Welcome messages that ID software and other system information

Demo

Update this slide if your
Demo doesn't cover
All of these anymore

Using Telnet and Netcat

- Very active
- ID a server
- ID a service

Countermeasures

Countermeasures

Misdirect

IIS lockdown tool

ServerMask

Speaking of misdirection

Learning Check

Learning Check

- **Active fingerprinting**
- **ServerMask**
- **Banner grabbing**
- **Passive fingerprinting**

Next Up:
Examining Vulnerability Scans