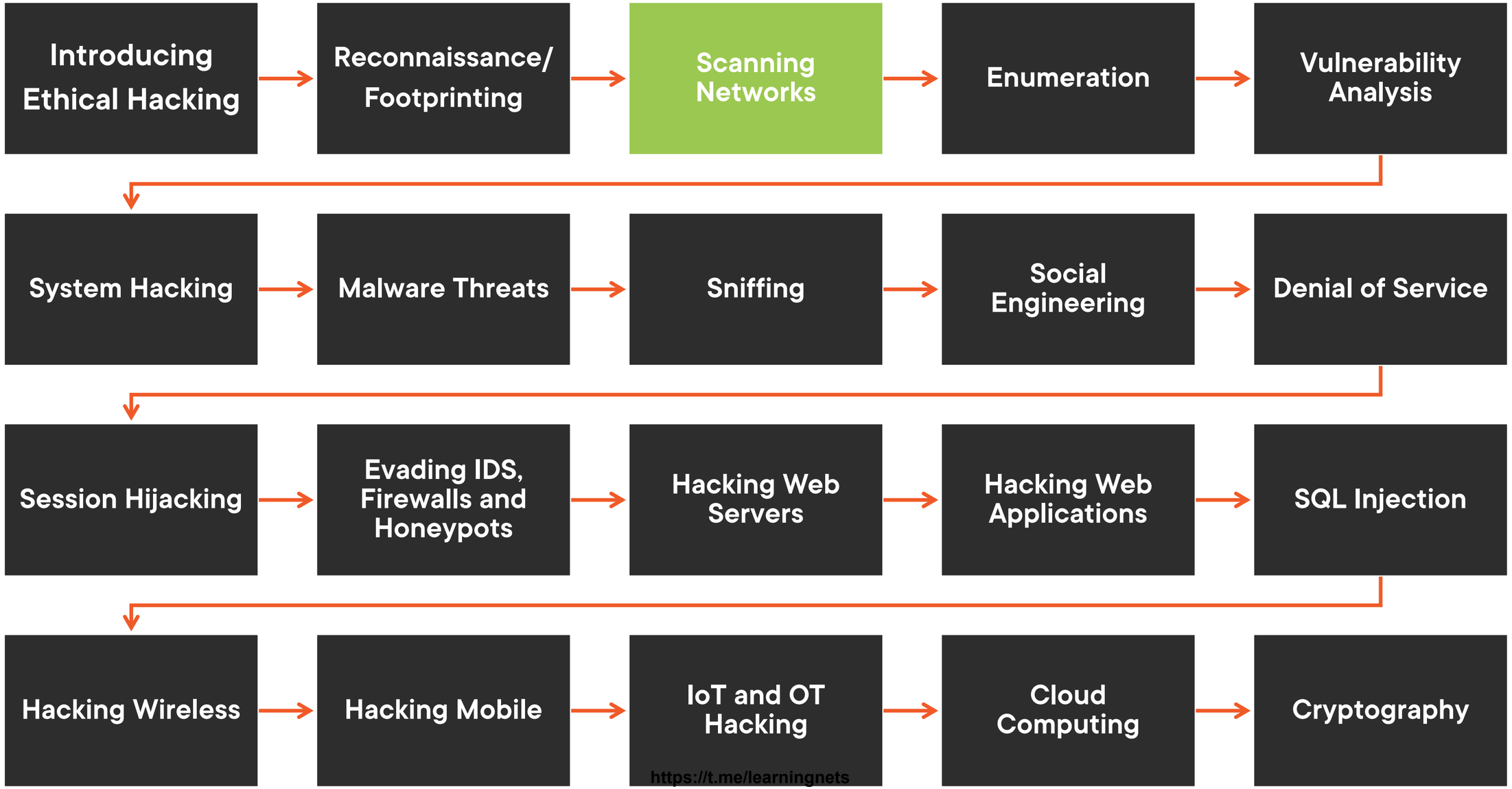
Ethical Hacking: Scanning the Network

Summarizing Scanning and It's Goals

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

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

Ethical Hacking Series



What is Scanning?

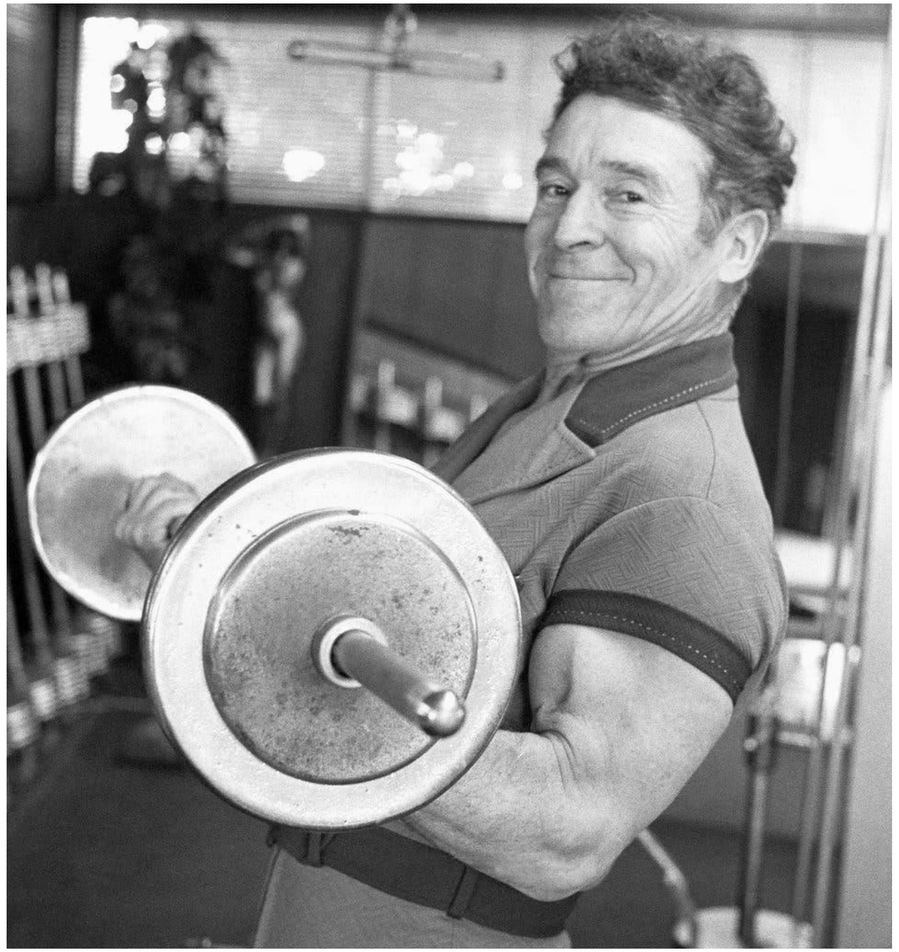
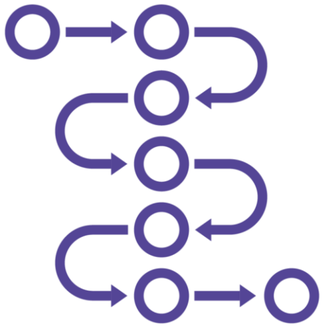


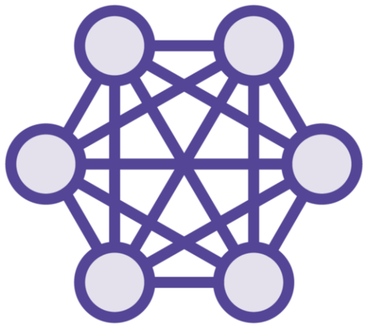
Photo credit: https://www.nytimes.com/2011/01/24/sports/24lalanne.html

We don’t know all the answers. If we did, we’d be bored. Keep looking, searching, trying to get more knowledge.

Jack LaLanne

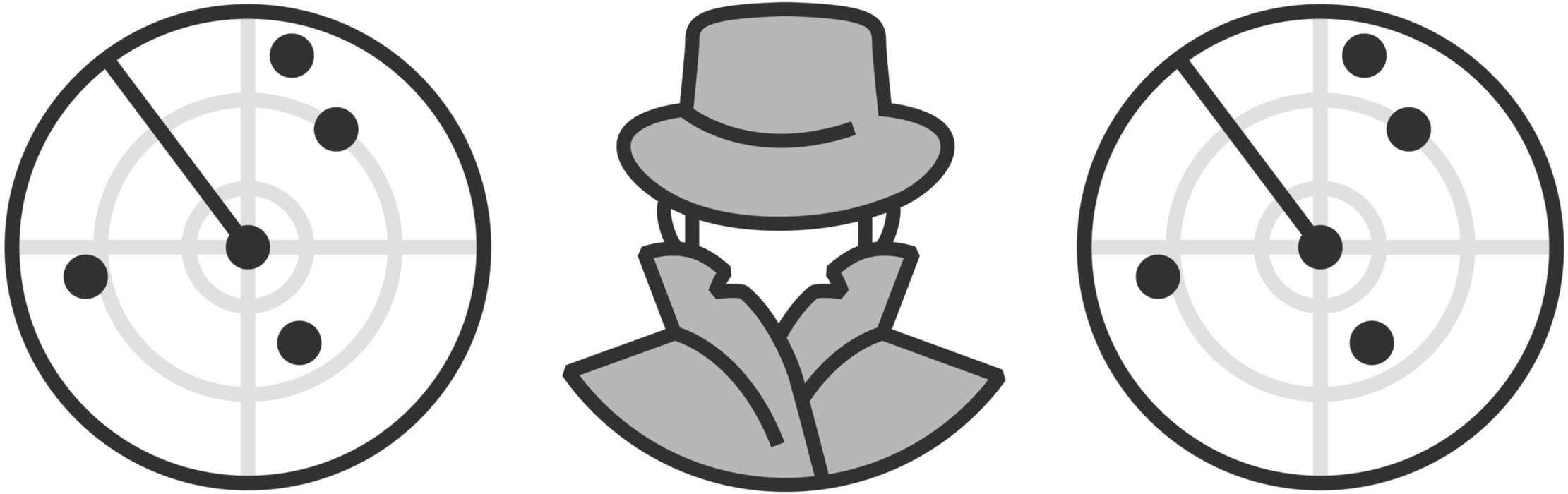
What is Scanning?



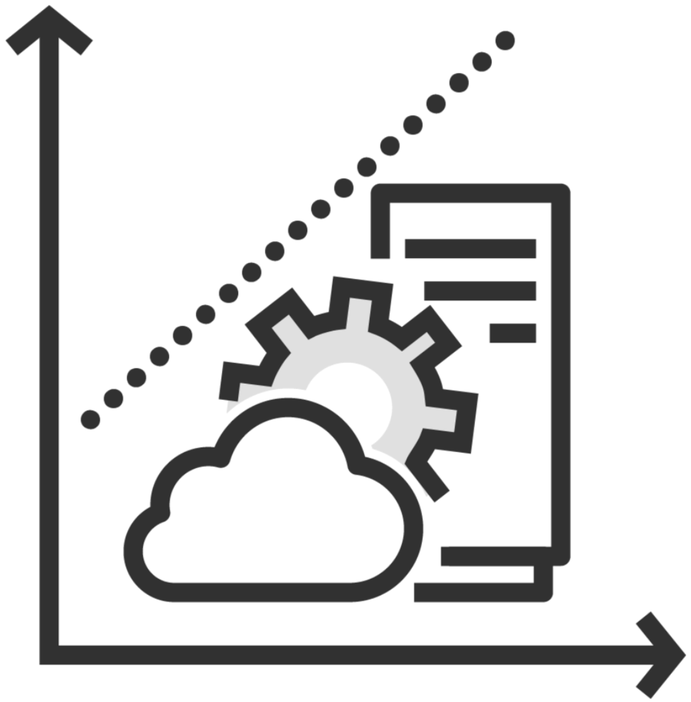


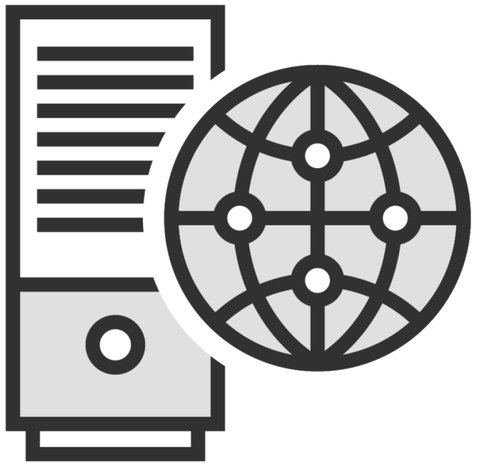
Scanning

A extended form of reconnaissance where the attacker learns more about their target. It is one of the most important phases of intelligence gathering for an attacker.



When Your Network Is Targeted





Always maintain a updated map of your network

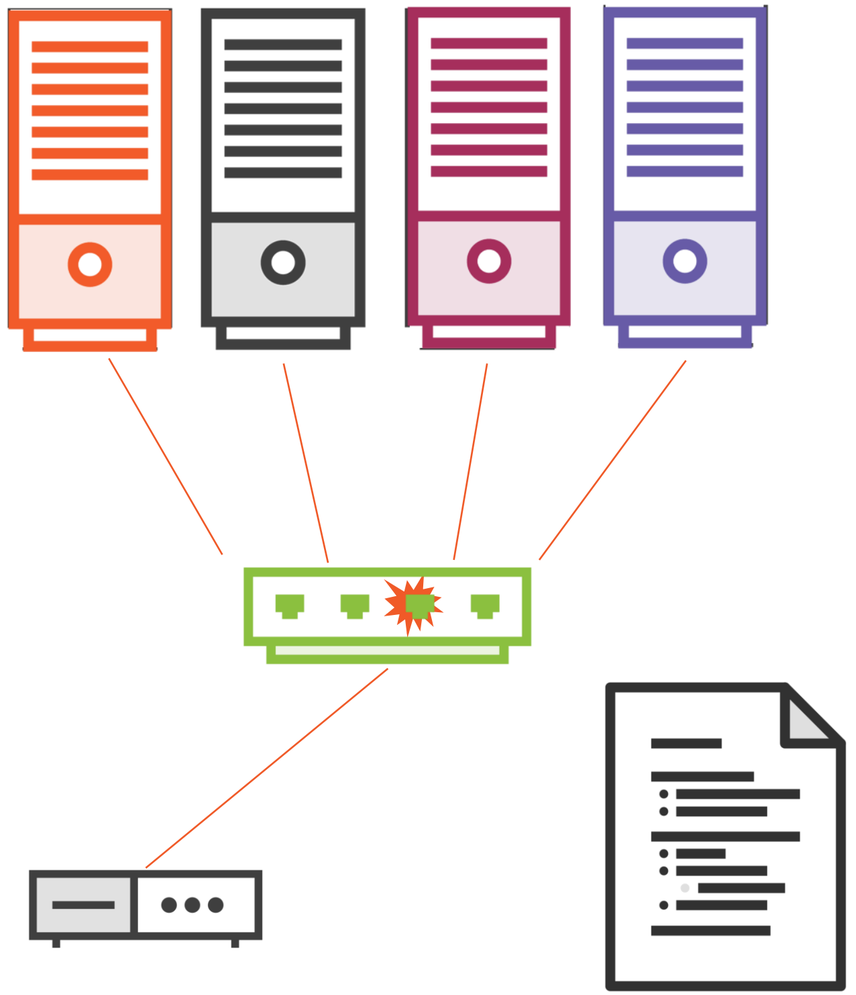
Types of Scanning

Network Scan

Identify active hosts

Identify operating systems

Identify IP addresses



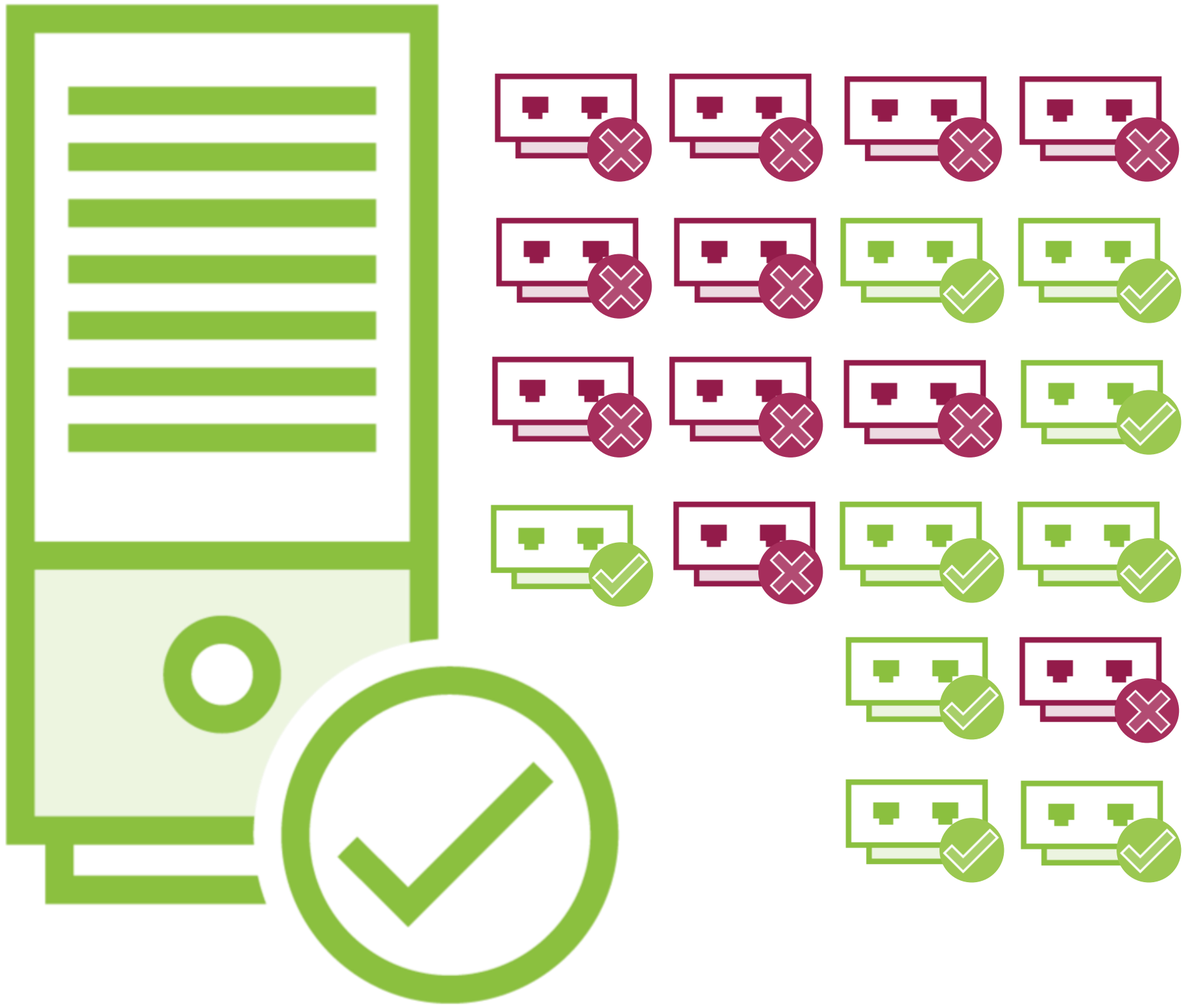
Network Scan

A procedure for identifying active hosts on a network, either to attack them or assess the security of the network.

What Is a Port?

192.168.0.15
IP Address
+
HTTP
Protocol
192.168.0.15:80

Port Scan



Which ports are responding?

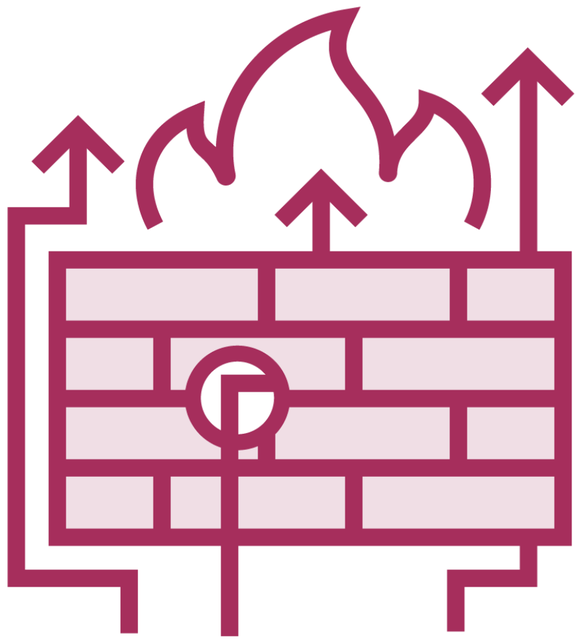
Which services use those ports?

Port Scan

As the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in.

It involves connecting to or probing TCP and UDP ports of the target system to determine whether the services are running or are in a listening state.

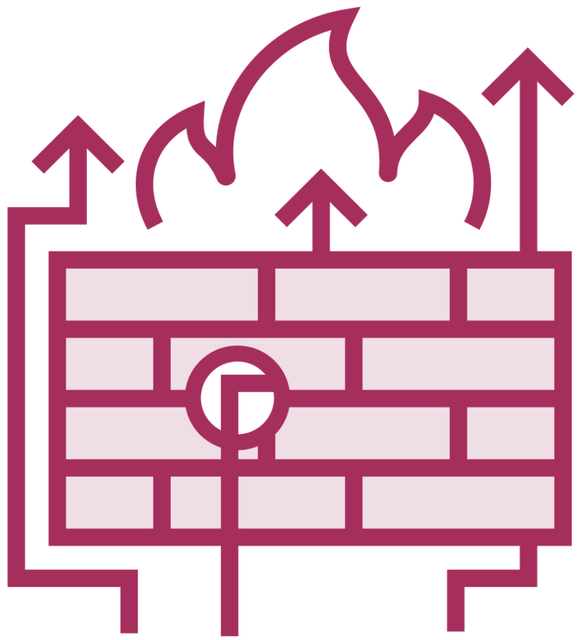
Vulnerability Scan



IT Professionals should conduct vulnerability scans periodically to identify threats in their own environment

Identified issues can easily be fixed through updated security patches

Vulnerability Scan



A method for checking if a system is exploitable by identifying its vulnerabilities

Scans a catalog of common files with known vulnerabilities and common exploits for a range of servers

Searches for backup files or directory traversal exploits

What's the Goal?

Objectives of Scanning

Discover the network's live hosts, IP addresses, and open ports

Objectives of Scanning

Discover the network's live hosts, IP addresses, and open ports

Discover the OS and system architecture of the target

Discover the services running/listening on the target system

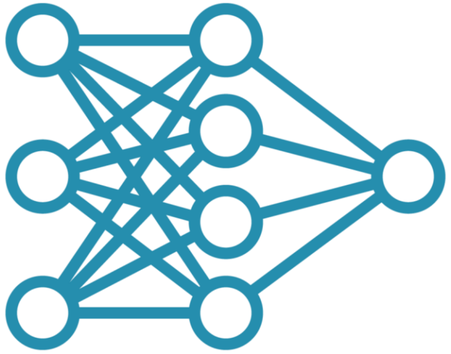
Identify specific applications or versions of a particular service

Identify vulnerabilities in any of the network systems

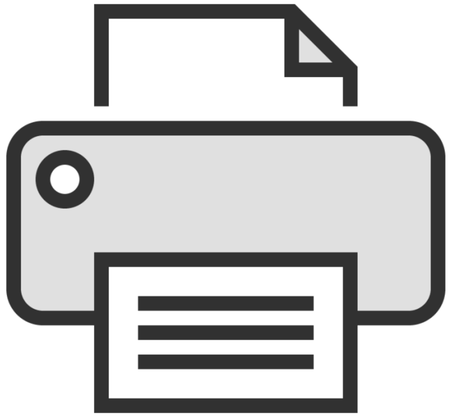
Scanning is another form of reconnaissance as it is all about gathering information

What Techniques Are Used?

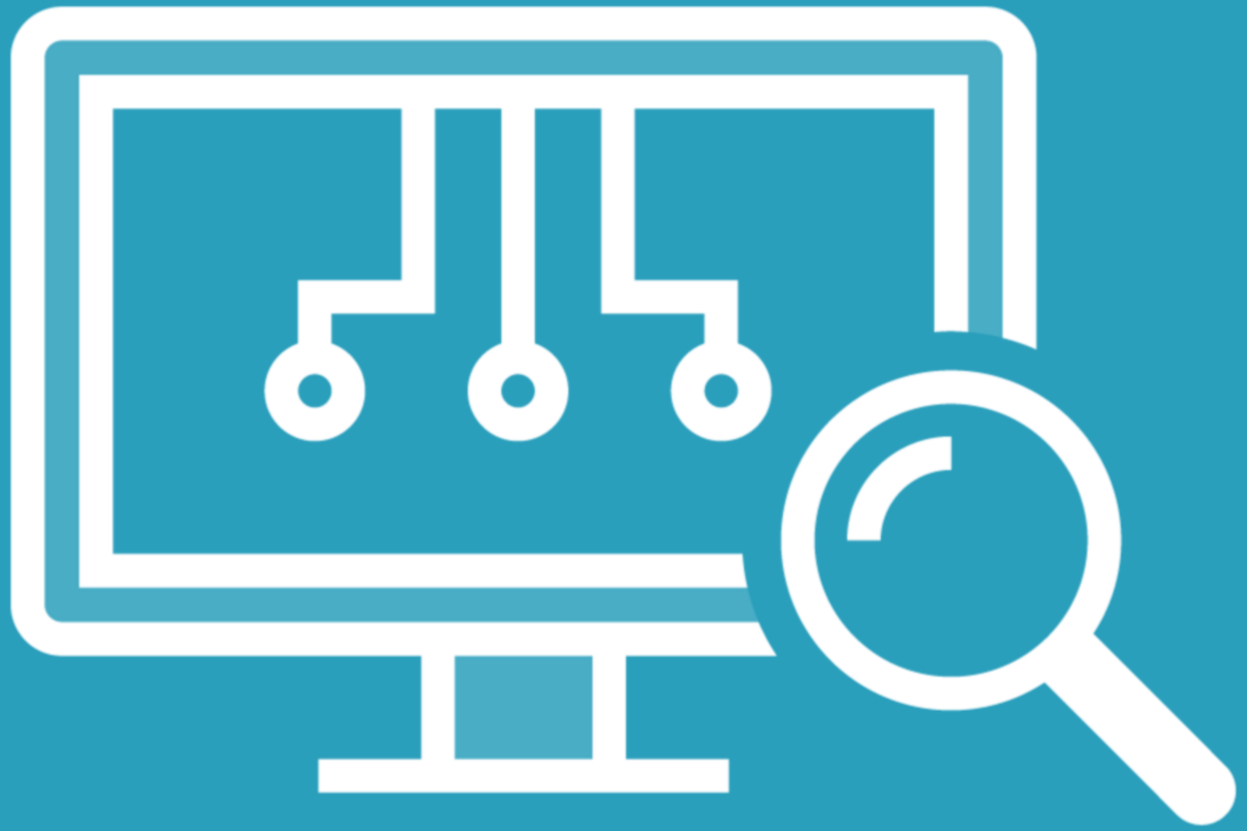
Scanning Techniques



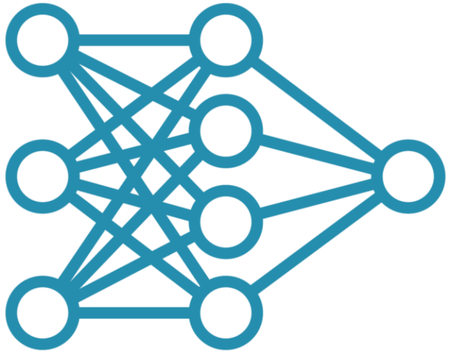
Internal or External



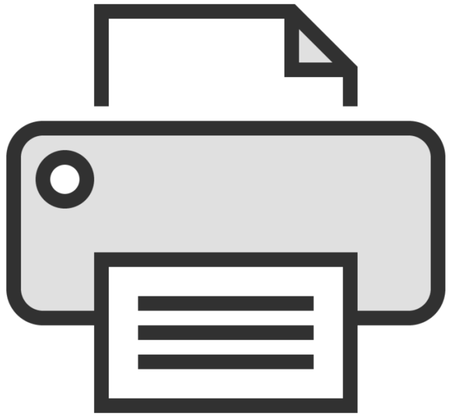
Not just computers



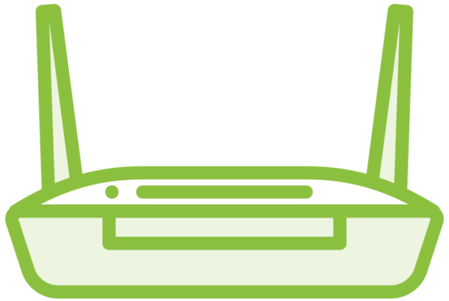
Scanning Techniques



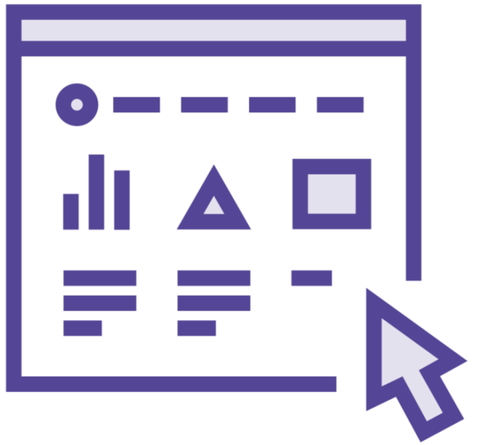
Internal or External



Not just computers



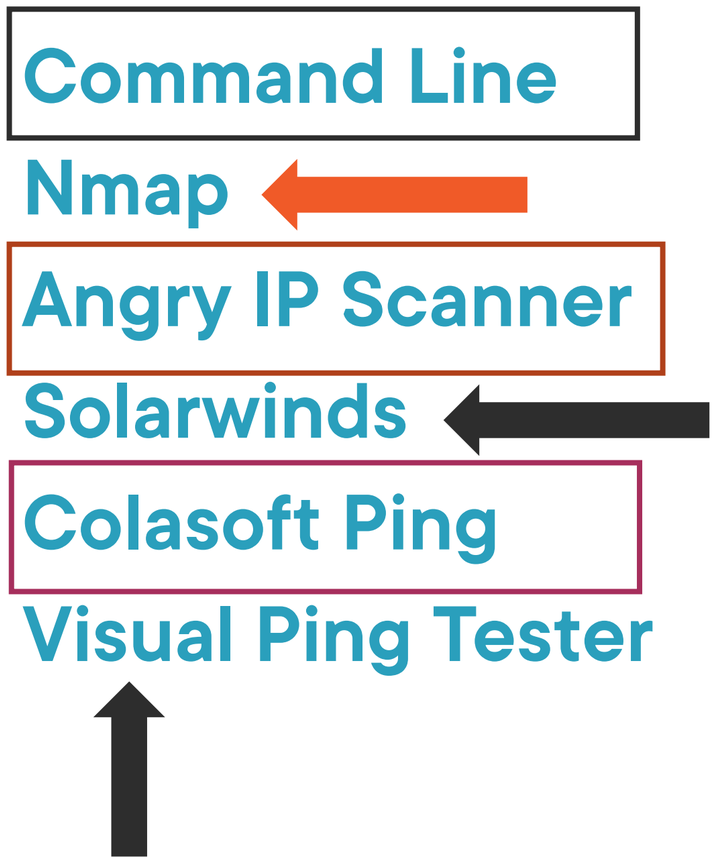
Don’t forget Wi-Fi



Banner Grabbing

What Tools Are Used?

Scanning Tools



Ping Scanner Pro
Ping Sweep
Ping Monitor
Pinkie
PingInfoView
PacketTrap MSP

GFI
SoftPerfect
Nessus
NetStumbler
Ping Tester
The list keeps going

Learning Check

Learning Check

- **Vulnerability scan**
- **Network scan**
- **Noisy**
- **Gather information**
- **Port scan**

Next Up:
Understanding the 3-Way Handshake