Pen Testing with Bash

Network Reconnaissance and Enumeration

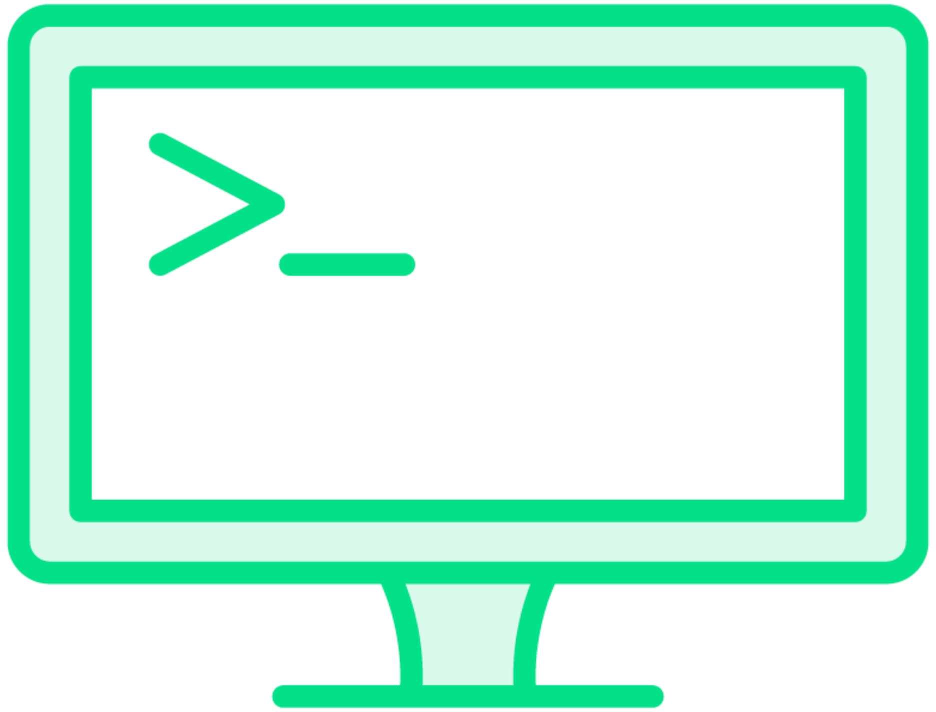
Malek Mohammad

Information Security Consultant

https://github.com/malek-mohammad
www.linkedin.com/in/malekmohammad

Reconnaissance

Information Gathering	VS	Enumeration
Passive info gathering		Active scanning
Help in testing planning		Use of tools
From public sources		Identify attack vectors



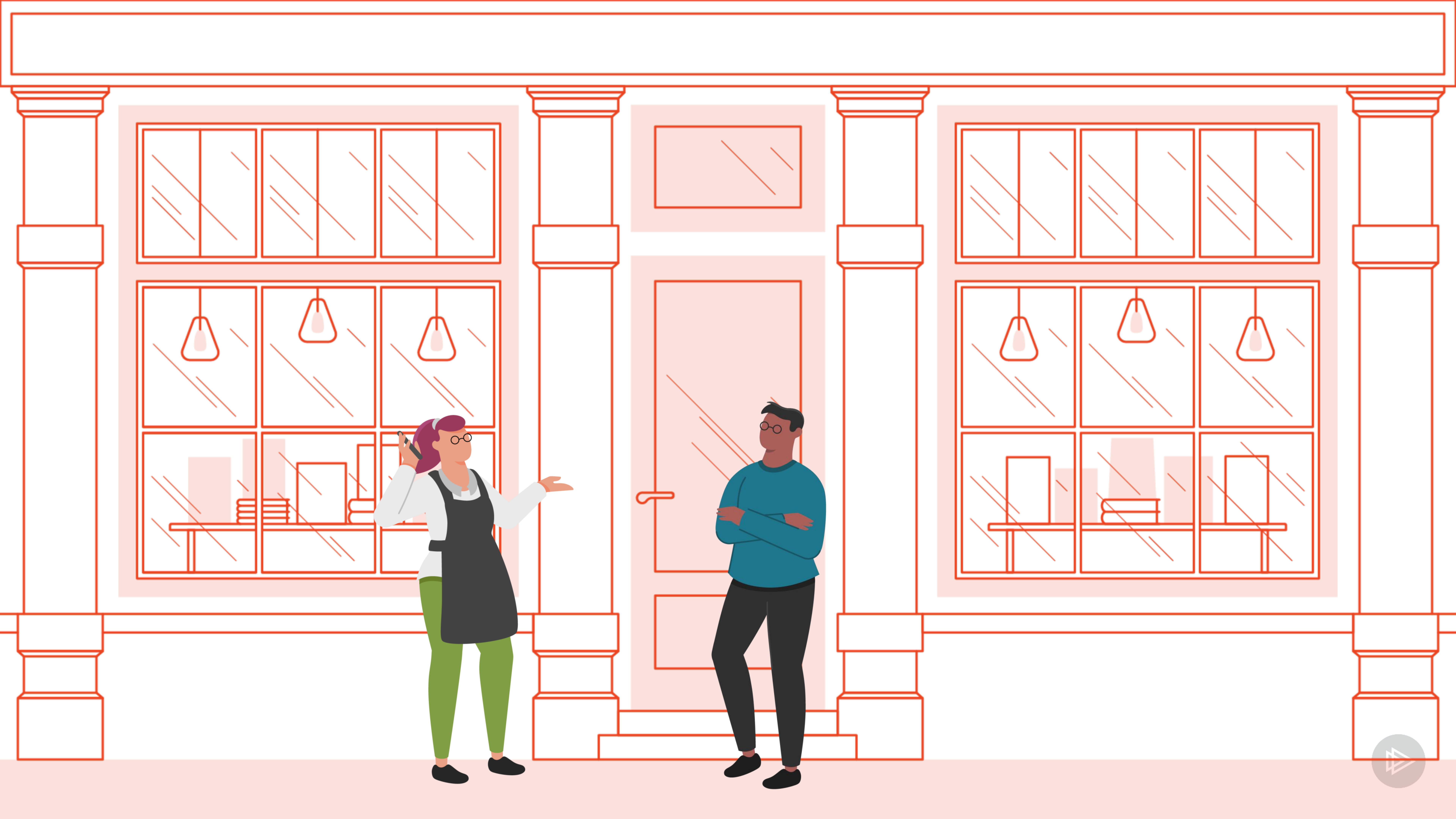
More than just commands

Tons of functionality

Essential for pen testers

Widely available

Resource rich

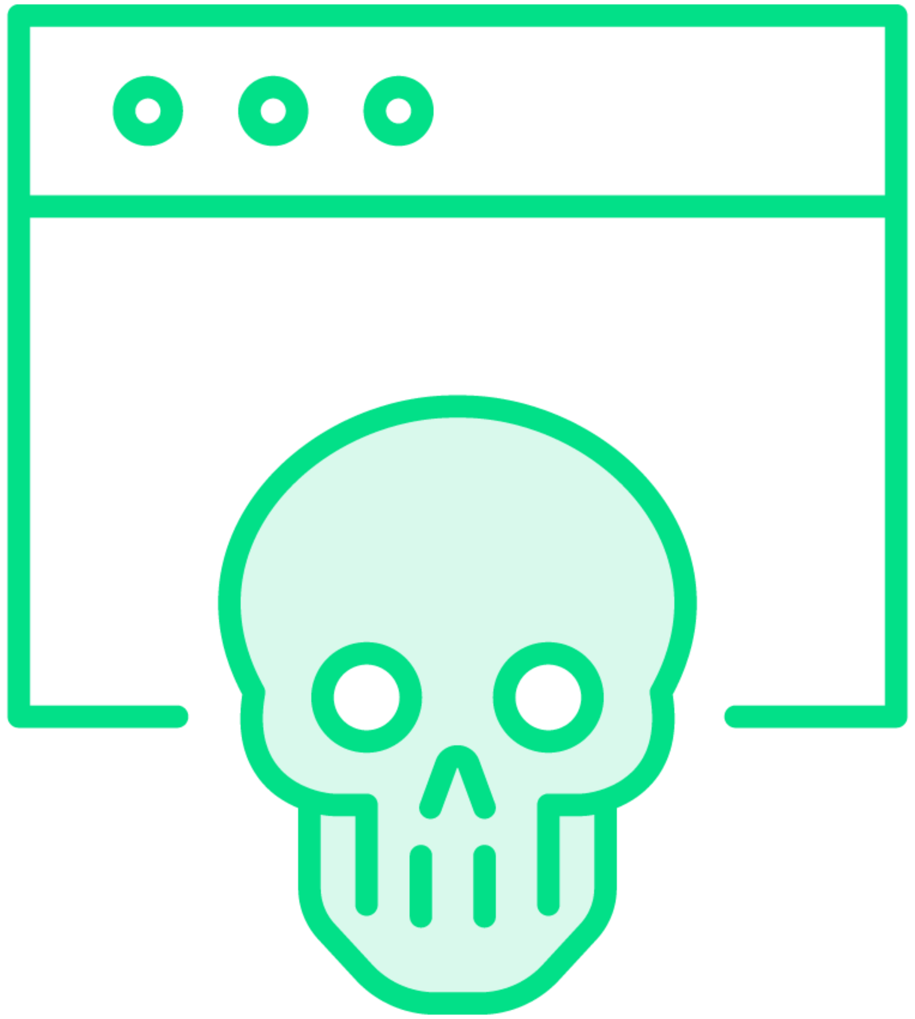


Early engagement

Registration database

Publicly available

Info query



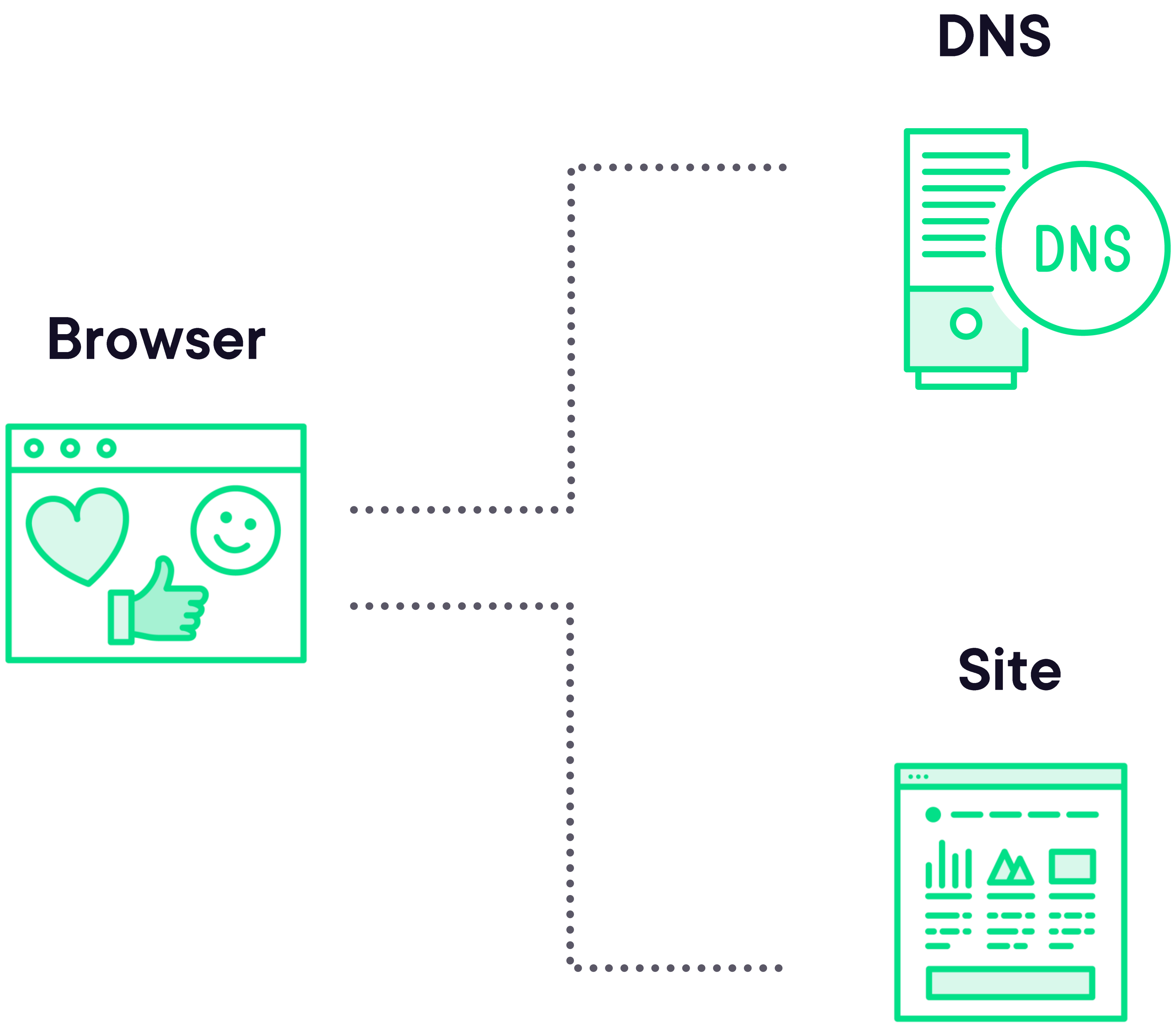
Compile Information

Analyze Data

Identify Weakness

Translates domain name to IP address

Making internet usage easier



DNS

Browser

Site

Host to IP mapping

Reverse DNS lookup

Mail server

Text records

A records handle mapping domain names to IPs

MX records specifies mail servers

CNAME records do domain name to domain name mapping

TXT records store textual data related to the domain name

NS records specify DNS servers

Interrogation tool

It has all the needed functions

It is prevalent

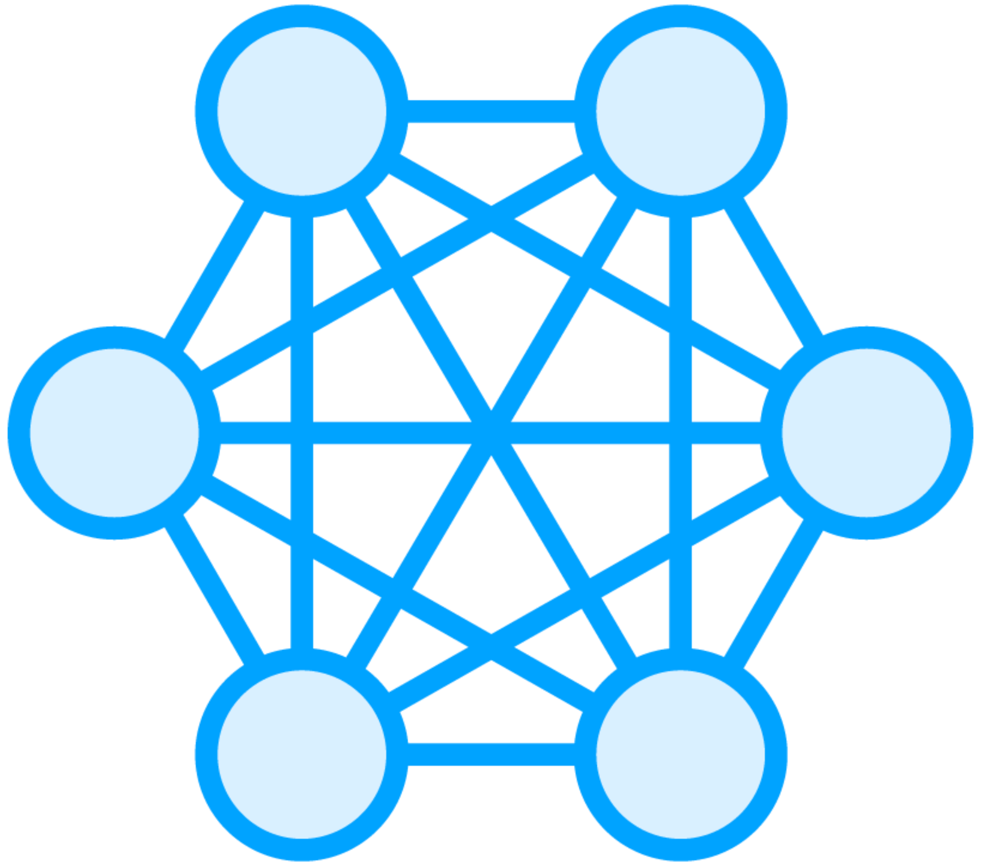
Get the list of subdomains

Bigger attack surface

DNSMap is the tool for you

Discovery is done by brute forcing

Uses a wordlist for subdomains



IP to MAC mapping

Can be used for discovery

Bound to local network

ARP vs ICMP

- Stealthy in nature
- More reliable

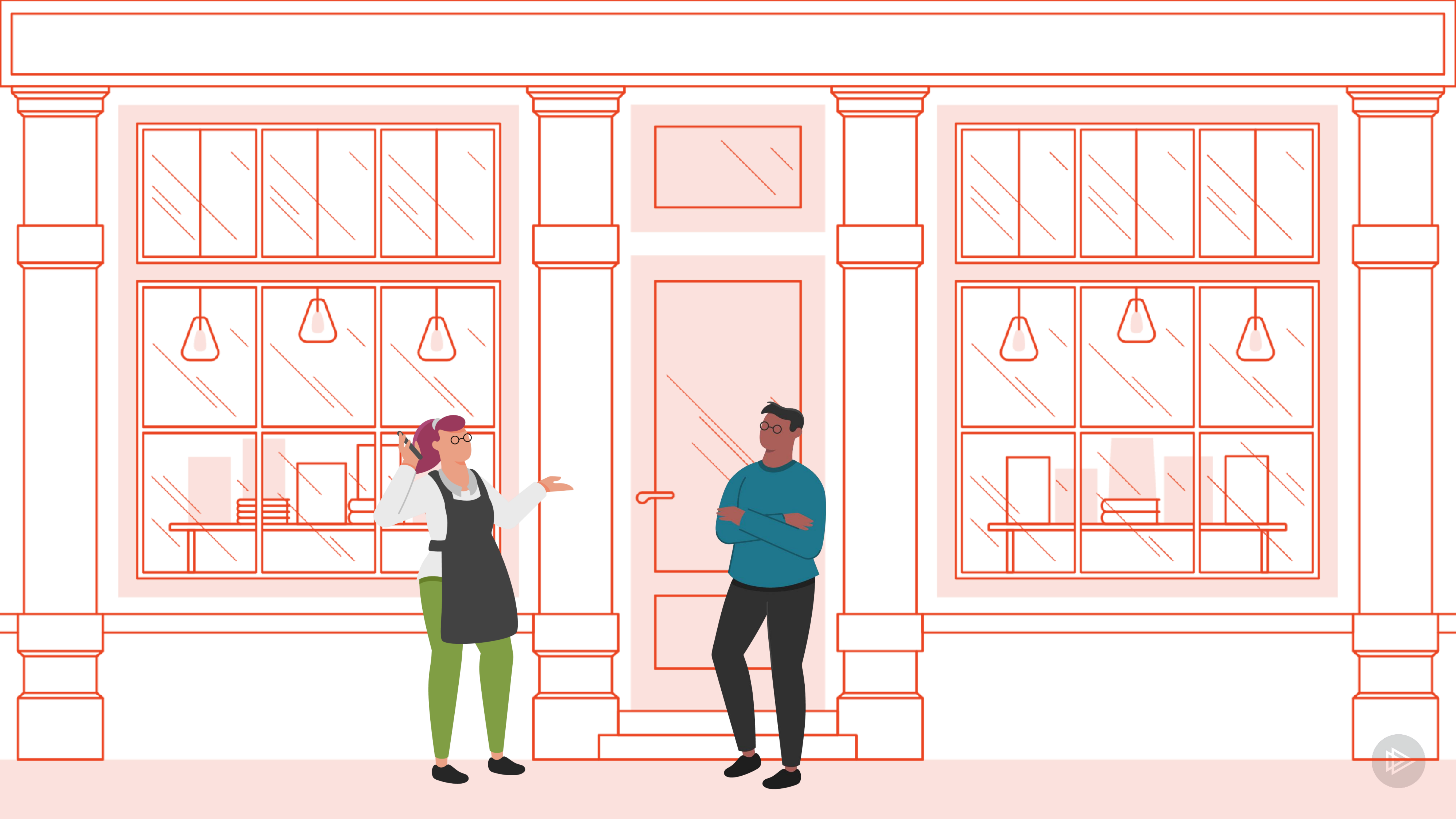
Open-source tool

Equipped with functionality

Network scanning capability

ARP does not always work

Utilize a combination of scan types



Costly and error prone

Bash scripts streamline your work

Get an accurate result quickly